

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 24.Dec.03		3. REPORT TYPE AND DATES COVERED THESIS
4. TITLE AND SUBTITLE ADDRESSING SECURITY CONCERNS IN THE EARLY STAGES OF THE PROJECT LIFECYCLE"			5. FUNDING NUMBERS	
6. AUTHOR(S) 1ST LT MATTHEWS BENJAMIN E				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) UNIVERSITY OF TEXAS AT AUSTIN			8. PERFORMING ORGANIZATION REPORT NUMBER CI02-1339	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) THE DEPARTMENT OF THE AIR FORCE AFIT/CIA, BLDG 125 2950 P STREET WPAFB OH 45433			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION AVAILABILITY STATEMENT Unlimited distribution In Accordance With AFI 35-205/AFIT Sup 1			12b. DISTRIBUTION CODE DISTRIBUTION STATEMENT A Approved for Public Release Distribution Unlimited	
13. ABSTRACT (Maximum 200 words)				
20040121 046				
14. SUBJECT TERMS			15. NUMBER OF PAGES 192	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT	

**ADDRESSING SECURITY CONCERNS IN THE EARLY
STAGES OF THE PROJECT LIFECYCLE**

by

Benjamin Earl Matthews, B.S.

Thesis

Presented to the Faculty of the Graduate School of
The University of Texas at Austin
in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science in Engineering

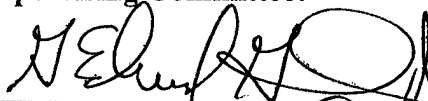
The University of Texas at Austin

December 2003

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

**ADDRESSING SECURITY CONCERNS IN THE EARLY
STAGES OF THE PROJECT LIFECYCLE**

Approved by
Supervising Committee:



Supervisor: G. Edward Gibson, Jr.



Co-Supervisor: Stephen R. Thomas

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government

Abstract

ADDRESSING SECURITY CONCERNS IN THE EARLY STAGES OF THE PROJECT LIFECYCLE

Benjamin Earl Matthews, M.S.E.

The University of Texas at Austin, 2003

Supervisor: G. Edward Gibson, Jr.

This thesis is a starting point to develop best practices for project security on industrial projects. It is a result of input from 17 industry professionals working in a committee setting over a one-year period. The thesis outlines a methodology for updating best practices to include security. It shows how to address security early in the project lifecycle and the implications towards the capital facility delivery process. Finally, recommended updates to existing Construction Industry Institute (CII) best practices are provided as well as recommendations to the United States Air Force and industry. The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or the U.S. Government.

Acknowledgements

I would like to thank my supervisor, Dr. G. Edward Gibson, Jr. and co-supervisor Dr. Stephen R. Thomas for guiding me throughout this research process. I would also like to thank Bob Chapman, Ph.D. of the National Institute of Standards and Technology and all the members of the Steering and Practice Development teams. This thesis is the result of all their inputs over the last year. Finally, I would like to thank the United States Air Force for giving me the opportunity to advance my education at the University of Texas.

December 5, 2003

Table of Contents

List of Tables.....	xi
List of Figures	xii
Chapter 1: Introduction	1
1.1. Purpose.....	1
1.2. Construction Industry Institute.....	1
1.3. Scope	3
1.4. Objectives.....	4
1.5. Thesis Organization.....	4
Chapter 2: Background.....	5
2.1. Definitions and Descriptions.....	5
2.1.1. Security.....	5
2.1.2. Threat	6
2.1.3. Consequences	8
2.1.4. Risk/Vulnerability Assessment	10
2.2. Major Terrorism Events	12
2.3. Industry Vulnerabilities.....	14
2.3.1. Overview	14
2.3.2. Example Vulnerabilities.....	15
2.4. Pre 9/11 Threat Response.....	17
2.5. Post 9/11 Threat Response	19
2.5.1. Department of Homeland Security.....	20
2.5.2. National Strategy for Homeland Security	21
2.5.3. Physical Protection of Critical Infrastructure and Key Assets	22
2.5.4. Public/Private Partnerships	23
2.5.5. Industrial Specific Guidelines	24

2.6.	Department of Defense Responses to 9/11	25
2.7.	Project Lifecycle	26
2.8.	Summary	27
Chapter 3: Research Methodology		29
3.1.	CII/NIST Study Overview	29
3.2.	Selection of Best Practices	30
3.3.	Best Practice Review Process	32
3.3.1.	Practice Update Example	32
3.3.2.	Process Flow Chart.....	33
Chapter 4: Security Updates.....		35
4.1.	Pre-Project Planning.....	35
4.1.1.	Practice Overview	35
4.1.2.	Implications of Pre-Project Planning to the Project Delivery Process and Security.....	36
4.1.3.	Update to Pre-Project Planning Handbook	37
4.1.4.	Update to PDRI	38
4.2.	Alignment.....	40
4.2.1.	Practice Overview	40
4.2.2.	Implications of Alignment to the Project Delivery Process and Security.....	41
4.2.3.	Update to Alignment	42
4.3.	Design Effectiveness	44
4.3.1.	Practice Overview	44
4.3.2.	Implications of Design Effectiveness to the Project Delivery Process and Security.....	45
4.3.3.	Update to Design Effectiveness	45
4.4.	Constructability	47
4.4.1.	Practice Overview	47
4.4.2.	Implications of Constructability to the Project Delivery Process and Security.....	47

4.4.3. Update to Constructability	48
4.5. Materials Management.....	49
4.5.1. Practice Overview	49
4.5.2. Implications of Materials Management to the Project Delivery Process and Security.....	50
4.5.3. Update to Materials Management	51
4.6. Job Site Security.....	52
4.6.1. Practice Overview	52
4.6.2. Implications of Job Site Security to the Project Delivery Process and Security.....	52
4.6.3. Update to Job Site Security	53
4.7. Planning For Startup.....	53
4.7.1. Practice Overview	53
4.7.2. Implications of Planning for Startup to the Project Delivery Process and Security.....	54
4.7.3. Update to Planning for Startup.....	55
4.8. Summary	56
Chapter 5: Conclusions and Recommendations.....	58
5.1. Conclusions	58
5.2. Recommendations	59
5.2.1. Recommendations to Industry.....	59
5.2.2. Recommendations to CII.....	60
5.2.3. Recommendations to United States Air Force	61

Appendix A: Committee Membership	63
Appendix B: Practice Development Team Meeting Agendas	64
Appendix C: Pre-Project Planning Handbook Updates	70
Appendix D: PDRI Updates	79
Appendix E: Alignment Updates	96
Appendix F: Design Effectiveness Updates	104
Appendix G: Constructability Updates	108
Appendix H: Materials Management Updates	116
Appendix I: Job Site Security Guidelines	138
Appendix J: Planning for Startup Updates	141
Appendix K: Security Matrix	169
Appendix L: DoD UFC guidelines	174
Glossary	175
Bibliography	177
Vita	180

List of Tables

Table 1: CII Knowledge Areas (CII 2002).....	2
Table 2: Practice Development Team Threat levels	8
Table 3: Practice Development Team Consequence levels	10
Table 4: Critical Infrastructure Sectors (Bush 2003)	22
Table 5: Subject Matter Experts.....	32
Table 6: Constructability Concepts (CII 1993)	48
Table 7: Startup Planning Model Phases and Activities (CII 1998)	54

List of Figures

Figure 1: DHS Threat Levels	7
Figure 2: Oil System Vulnerabilities (NRC 2002).....	16
Figure 3: Public-private partnerships in US Critical Infrastructures (Erwann 2003).....	19
Figure 4: Ability to Influence Final Cost over Project Life (CII 1986)	27
Figure 5: Applicability versus Impact of Best Practices (Sylvie 2003)	31
Figure 6: Applicability versus Impact of Proposed Best Practices (Sylvie 2003).....	31
Figure 7: Process Flow Chart for Developing Security Best Practices.....	34
Figure 8: Cost vs. Influence curves for the Project Lifecycle (CII 1996).....	37
Figure 9: Example updates to Pre-Project Planning Handbook (changes in bold)	38
Figure 10: Example updates to PDRI Elements (changes in bold)	39
Figure 11: 3-D Schematic Organizational Alignment for a Project (CII 1997)....	40
Figure 12: Example updates to Alignment (changes in bold)	43
Figure 13: Example updates to Design Effectiveness (changes in bold)	46
Figure 14: Example updates to Constructability (changes in bold)	49
Figure 15: Example updates to Materials Management (changes in bold)	51
Figure 16: Example updates to Job Site Security Guidelines	53
Figure 17: Example updates to Planning for Startup (changes in bold).....	56
Figure 18: Security Matrix example.....	57

Chapter 1: Introduction

1.1. PURPOSE

Over the past two years since the September 11th attacks, security concerns have come to the forefront in industrial projects and facilities. Security includes all measures taken to guard against malevolent, intentional acts, both internal and external, which result in adverse impacts. Varying security measures are needed on industrial projects to respond to the known and unknown threats. Currently, there are many different organizations characterizing threats, but very few have published recommended actions or processes to address security. The purpose of this thesis is to develop best practices for use during project delivery that will improve security throughout the project lifecycle. This thesis will serve as a framework for companies to understand and respond to threats to the industry and their associated consequences.

Another purpose is to show how to address security in the beginning of the project lifecycle through the use of existing Construction Industry Institute (CII) best practices. Job site security, which is not covered in the CII practices, is also addressed.

1.2. CONSTRUCTION INDUSTRY INSTITUTE

The Construction Industry Institute (CII) is a unique consortium of leading owners and contractors who joined together in 1983 with academia to find better ways of planning and executing capital construction programs, through research, and to benefit by the application of that knowledge to their work. The mission

of CII is, “to improve the business effectiveness of the capital facilities life cycle, including safety, quality, schedule, cost, security, reliability, and operability. Participation in CII provides members the opportunity for a competitive advantage in the global marketplace” (CII 2002).

The overall body of knowledge for CII is arranged in a topological form called the Knowledge Structure. There are 13 Knowledge Areas that are logical groupings of topics that reflect project phases or construction issues. The Knowledge Areas are listed in Table 1:

Table 1: CII Knowledge Areas (CII 2002)

• Front-End Planning	• Design
• Procurement	• Project Processes
• Project Controls	• Contracts
• Construction	• Startup and Operations
• People	• Organization
• Safety, Health, and Environmental	• Information/Technology Systems
• Globalization Issues	

CII is the leading developer of industry best practices to improve the effectiveness of the capital project delivery process and currently has identified 13 that will be discussed later in this document. A CII Best Practice is defined as a process or method that, when executed effectively, leads to enhanced project performance (CII 2001). CII through its Benchmarking & Metrics activity has extensive experience in the benchmarking of best practices. CII has the largest publicly accessible database for benchmarking best practices. Through this

study, the intention is that security will eventually be added as a best practice and appropriately benchmarked.

1.3. SCOPE

The scope of this research focuses on the National Institute of Standards and Technology (NIST) funded study for CII to develop best practices related to the security of capital facilities projects. The research only covers industrial projects to include chemical manufacturing, oil production and refining, natural gas processing and distribution, and power generation and distribution. Seventeen industry professionals worked in a committee setting to examine existing CII best practices in order to develop a security best practice. The author was a member of the research team with a primary role of ensuring that the team was aware of any parallel efforts that pertained to security on industrial projects and assisting in the development effort. The research updated existing CII literature covering the pre-project planning, design, procurement, construction, and startup phases of capital projects. These updates and security issues will be discussed in more detail later in the thesis. Future research will determine how the concepts discussed in this thesis apply to other industry groups besides industrial.

1.4. OBJECTIVES

The objectives of this thesis are therefore to:

1. Summarize homeland security literature as it pertains to industrial projects
2. Determine and adapt applicable CII best practices to develop a security best practice
3. Provide recommendations for industry implementation

1.5. THESIS ORGANIZATION

The organization of this thesis begins with background on security and various efforts that took place before and after September 11th, 2001 in Chapter 2. Then there is a review of the research methodology in Chapter 3. Details of how the CII best practices were selected are provided, including a process flow chart that shows an overview of the study. Chapter 4 describes the updates that the Practice Development team made to the best practices. It contains an overview of the practice, implications to the project delivery process, and sample updates. Finally, Chapter 5 provides conclusions and recommendations. All of the security upgrades to the various CII Best Practices are given in the Appendices.

Chapter 2: Background

This chapter presents background information on security, terrorism, threats, and the responses to those threats. The information was collected through a literature review of publications, GAO reports, conference proceedings, online journals, and email news services.

2.1. DEFINITIONS AND DESCRIPTIONS

2.1.1. Security

Although there are many definitions of security, the Practice Development team adapted a definition from Webster's dictionary to fit the scope of research.

Security includes all measures taken to guard against malevolent, intentional acts, both internal and external (e.g., sabotage, crime, and attack), that result in adverse impacts such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and offsite effects (consequence).

Security can be classified into three major categories: Physical, Personnel and Information. Physical security involves equipment, building and grounds design and security practices designed to prevent physical attacks against facilities, people, property or information. There are four basic features of physical protection for buildings: the establishment of a secure perimeter, the prevention of progressive structural collapse, the isolation of internal threats from occupied spaces, and window glazing (Little 2002). Personnel security is mainly concerned with practices and procedures for hiring, terminations, and workplace issues and response. Screening procedures and background checks are also part

of personnel security. Information security consists of practices and procedures for protection of documents, networks, computer facilities and verbal communication. Firewalls, passwords, and a document control matrix are some examples of information security measures.

2.1.2. Threat

Threat is the first of two main considerations when determining security practices. Threat is defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset (API 2003). It is also the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

- Terrorists (international or domestic);
- Activists or pressure groups;
- Disgruntled employees or contractors;
- Criminals (e.g., white collar, cyber hacker, organized, opportunists).

Threat information is important reference data to allow the Owner/Operator to understand the adversaries interested in the assets of the facility, their operating history, their methods and capabilities, their possible plans, and why they are motivated. Adversaries may be categorized as occurring from three general types:

- Insider threats
- External threats
- Insiders working as colluders with external threats (API 2003)

The Department of Homeland Security (DHS) is the foremost authority to communicate national threat levels. On March 12, 2002, DHS initiated the threat level advisory system shown to the right in Figure 1. The Threat Conditions each represent an increasing risk of terrorist attacks. Each Threat Condition has suggested protective measures, but Federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures. Since the system has been activated, DHS raised and lowered the threat level between high and elevated six times (DHS 2003). As time continues to pass between terrorism events, it is critical that the nation takes these threat level adjustments seriously.

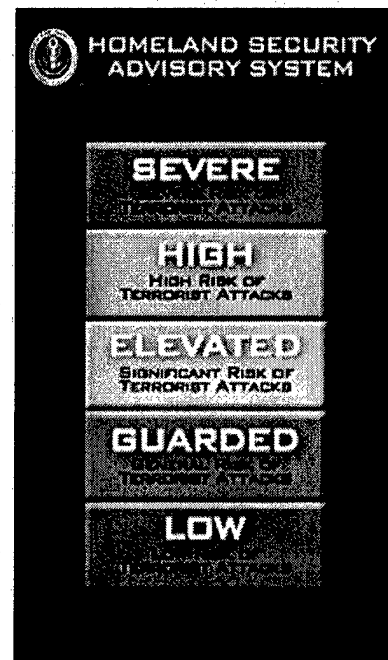


Figure 1: DHS Threat Levels

Very similar to the DHS, the Department of Defense has its own threat levels: Alpha, Bravo, Charlie, Delta (Delta being the highest). They are actually called Force Protection Conditions, but serve the same purpose as the DHS threat levels. Force Protection Conditions indicate the level of threat to military personnel in a given region. The Practice Development Team developed threat level rankings for industrial projects shown on the next page in Table 2. These rankings are adapted from American Petroleum Institute methodology (API 2003). The table provides a clear threat definition level based on the type of threat, the capability and intent to attack, and the assets targeted.

Table 2: Practice Development Team Threat levels

Category	Description
5 - Very High	Indicates that a definite threat exists against the asset and that the adversary has both the capability and intent to launch an attack or commit a criminal act, and that the subject or similar assets are targeted on a frequently recurring basis.
4 - High	Indicates that a credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack or commit a criminal act against the asset, based on related incidents having taken place at similar assets or in similar situations.
3 - Medium	Indicates that there is a possible threat to the asset based on the adversary's desire to compromise similar assets and/or the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents.
2 - Low	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the asset.
1 - Very Low	Indicates no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets.

2.1.3. Consequences

According to the Center for Chemical Process Safety, consequences are defined as, "the amount of loss or damage that can be expected, or may be expected from a successful attack against an asset" (CCPS 2002). Consequences are used as one of the key factors in determining the criticality of an asset or facility and the degree of security countermeasures required. Some examples of relevant consequences include:

- Injuries to the public or to workers

- Environmental damage
- Direct and indirect financial losses to the company and to suppliers and associated businesses
- Disruption to the national, regional or local operations and economy
- Loss of reputation or business viability
- Evacuation of people living or working near the facility
- Excessive media exposure and related public hysteria affecting people that may be far removed from the actual event location

The Practice Development team developed consequence level rankings for industrial projects shown on the next page in Table 3. Similar to the threat levels in the previous section, these rankings are also adapted from American Petroleum Institute methodology (API 2003). The consequence levels use key words like “extensive”, “significant”, “moderate”, and “minor” to distinguish the categories. The table also uses the possibility of offsite or onsite injuries to clarify the consequence levels. During a project, the project team evaluates the threat levels and consequence levels as a part of the Risk/Vulnerability Assessment. Details of the Vulnerability Assessment are covered in the next section.

Table 3: Practice Development Team Consequence levels

Category	Description
5 – Very Severe	<ul style="list-style-type: none"> • Possibility of any offsite fatalities; possibility for multiple onsite fatalities • Extensive environmental impact onsite and/or offsite • Extensive property damage • Very long term business interruption/expense
4 - Severe	<ul style="list-style-type: none"> • Possibility of any offsite injuries; possibility for onsite fatalities • Significant environmental impact onsite and/or offsite • Significant property damage • Long term business interruption/expense
3 - Moderate	<ul style="list-style-type: none"> • No offsite injuries; possibility for widespread onsite injuries • Moderate Environmental impact onsite and/or offsite • Moderate Property damage • Medium term business interruption/expense
2 - Minor	<ul style="list-style-type: none"> • Possibility for onsite injuries • Minor Environmental impact onsite only • Minor Property damage • Short-term business interruption/expense
1 – Very Minor	<ul style="list-style-type: none"> • Possibility for minor onsite injuries • No Environmental impacts • Little/No Property damage • Little/No business interruption/expense

2.1.4. Risk/Vulnerability Assessment

A Security Vulnerability Assessment (SVA) is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact (CCPS 2002). SVAs are not a quantitative risk analysis, but are performed qualitatively using the best judgment of security

and safety professionals. The objective of conducting a SVA is to identify security hazards, threats, and vulnerabilities facing a facility, and to evaluate the countermeasures required to provide for the protection of the public, workers, national interests, the environment, and the company. The Threat and Consequence levels of the previous two sections are both critical pieces of the SVA. With this information, security risks can be assessed and strategies formed to reduce vulnerabilities.

The following items characterize the basic steps involved with virtually all vulnerability assessments:

- Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
- Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen;
- Identify potential security vulnerabilities that threaten the asset's service or integrity;
- Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur;
- Rank the risk of the event occurring and, make recommendations for lowering this risk;

- Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk to ensure adequate countermeasures are being applied (API 2003).

2.2. MAJOR TERRORISM EVENTS

The State Department defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience” (Council on Foreign Relations 2003). In another attempt to produce a definition, Paul Pillar, a former deputy chief of the CIA's Counterterrorist Center, argues that there are four key elements of terrorism:

- It is premeditated—planned in advance, rather than an impulsive act of rage
- It is political—not criminal
- It is aimed at civilians—not at military targets or combat-ready troops
- It is carried out by subnational groups—not by the army of a country (Council on Foreign Relations 2003)

The events listed below show that terrorism remains a significant threat to industrial projects. Whether the threat was internal or external, the consequences of each event could have been very tragic.

On March 28, 1979, the Three Mile Island nuclear plant had a minor malfunction in the secondary cooling circuit that caused the temperature in the primary coolant to rise. This event was not terrorism, but the sequence of the failure raised concerns about the possibility of future terrorist attacks. The rise

in primary coolant temperature caused the reactor to shut down automatically. At this point a relief valve failed to close, but instrumentation did not reveal the fact, and so much of the primary coolant drained away that the residual decay heat in the reactor core was not removed. The operators were unable to diagnose or respond properly to the unplanned automatic shutdown of the reactor. Deficient control room instrumentation and inadequate emergency response training proved to be root causes of the accident (World Nuclear Organization 2003). Although there were no deaths tied to this accident (which could easily have been intentional), it raised concerns about the consequences of nuclear plant failures.

On December 3, 1984 Methyl isocyanate (MIC) gas leaked from a Union Carbide India Limited (UCIL) pesticide plant in Bhopal, India, just after midnight. The Indian government reported that this incident resulted in approximately 3,800 deaths, 40 persons with permanent total disability, and 2,680 persons experiencing permanent partial disability. An independent investigation by Arthur D. Little, Inc. shows "with virtual certainty" that a disgruntled employee caused the Bhopal incident by introducing a large volume of water when he connected a water hose directly to the tank (Union Carbide Corporation 2002).

On January 22, 1991, Iraqi forces set two Kuwaiti oil refineries ablaze and then ignited the rest immediately before the coalition's ground troop attacks. Iraq hoped that the smoke would inhibit the operation of the coalition air forces and the movement of ground troops. Iraq's destruction of Kuwait oil production facilities devastated the Kuwait economy and created a major environmental

disaster (Rubin 2003). This was not a terrorist attack but it showed how an attack on an oil refinery could have severe consequences.

2.3. INDUSTRY VULNERABILITIES

In addition to the threats outlined in the previous section, there are many vulnerabilities in the nation's industrial infrastructure.

2.3.1. Overview

Terrorists target critical infrastructures to achieve three general types of effects:

- Direct infrastructure effects: Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.
- Indirect infrastructure effects: Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.
- Exploitation of infrastructure: Exploitation of elements of a particular infrastructure to disrupt or destroy another target (Bush 2003).

The statistics describing the nation's industrial infrastructure reflect a vast and highly decentralized industry. The U.S. is home to roughly 878,000 oil wells, 161 oil refineries, 726 gas-processing plants, 1,280,000 miles of natural gas pipeline, 220,000 miles of oil pipe, and 2,800 power plants according to the National Academy of Sciences (McFall 2003). Thousands of independent owners and operators are the driving force connecting these elements. According to the Environmental Protection Agency, 123 of the 15,000 U.S.

facilities that store or use chemicals could expose at least 1 million people to toxic gas if destroyed (Council on Foreign Relations 2003).

2.3.2. Example Vulnerabilities

At the end of 2002, the National Research Council published, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism." This book categorizes the vulnerabilities of industrial projects into three main areas: vulnerabilities of facilities, vulnerabilities of transmission lines, and vulnerabilities of the control systems (NRC 2002).

The chemical industry is vulnerable because terrorists have been known to use chemicals as weapons. Chemical weapons are readily available and have potential to inflict significant casualties. They are easily concealed and undetectable at a distance. Small amounts of chemical agents are used in enclosed places with great effect and delivered through postal, food or water supply networks. Terrorists can use toxic industrial chemicals by cutting pipes or opening valves. They may also hijack hazardous material transportation systems to use as weapons (NRC 2002).

The energy industry is critical because the United States relies upon their service to a great extent. With the technology boom of the late 1990's and its reliance upon electricity, the cost of power outages has increased from \$30 billion in 1995 to \$119 billion in 2001 (NRC 2002). Most recently, the August 14, 2003 blackout in the Northeast shut down the entire region for nearly two days. According to New York City comptroller William Thompson, this 29-hour

blackout cost the city \$1.05 billion, which is approximately \$36 million per hour (Reuters 2003).

Oil products also provide 97 percent of the energy to the transportation sector (NRC 2002). These systems are vulnerable because the majority of their infrastructure is outdoors and above ground. The delivery process is also more of a direct chain rather than an interconnected loop. An attack on an oil refinery or major electrical substation would severely disrupt the operations of society. Figure 2 below outlines sample vulnerabilities to the oil system.

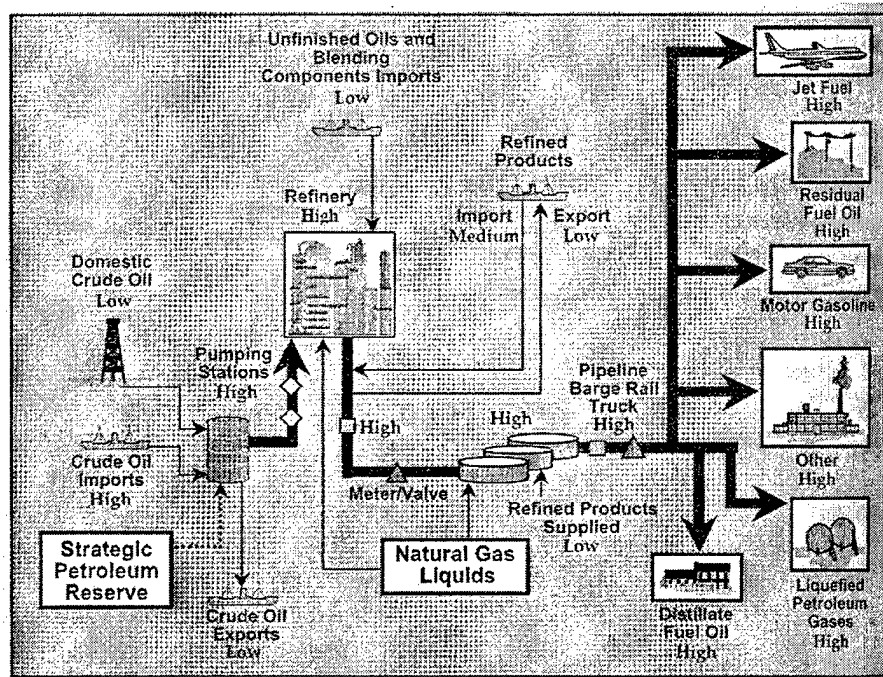


Figure 2: Oil System Vulnerabilities (NRC 2002)

The control systems of the above industries also represent vulnerabilities. Distribution systems are frequently remotely controlled, relying on supervisory control and data acquisition (SCADA) systems. To improve efficiency of

operations, there has been a rapid increase in the use of automation and computerization. Each industry relies heavily on information management and telecommunications systems (NRC 2002). As these trends continue to increase, the opportunities for cyber-attacks also increase.

Finally, the industry is also vulnerable to domestic terrorism attacks. The Patriot Act defines domestic terrorism as, "criminal acts dangerous to human life that appear intended to intimidate or coerce the civilian population or the government" (Tamaki 2003). Domestic terrorism also includes assassination, kidnapping or massive destruction of property aimed at affecting government conduct. The Oklahoma City Murrah Building bomb was an example of domestic terrorism.

The Earth Liberation Front (ELF) is one of a growing number of "eco-terrorist" groups that advocate "monkey-wrenching," a euphemism for acts of sabotage against industries and businesses perceived to be damaging the environment. In August 2003, the ELF set numerous Los Angeles Hummer vehicles on fire in order to "take the profit motive" away from those responsible for pollution. Damage estimates were over \$1 million (Tamaki 2003). The consequences in this case were monetary, but the consequences of a domestic terrorist attack to the chemical and oil industry could be much more severe.

2.4. PRE 9/11 THREAT RESPONSE

The first major legislation regarding critical infrastructure was the Presidential Decision Directive 63 (PDD 63) in May 1998. PDD 63 described a strategy for cooperative efforts by government and the private sector to protect

critical infrastructures. After assessing initial vulnerabilities, the directive initiated the second step of the process to build a national framework for "promoting national partnerships with different roles to play between governments and infrastructure owners to assess and manage new vulnerabilities from terrorism or malicious acts" (Erwann 2003). Such a global framework was recognized as essential to create a dynamic process of risk assessment and risk mitigation.

At the federal level, responsibilities within the departments and lead agencies as sector liaisons for protecting critical infrastructures were established. The Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC) were created in May 1998. On the industry side, organizations were also developed. The Partnership for Critical Infrastructure Security (PCIS) was established in December 1999, along with Information Sharing and Analysis Centers (ISACs), which are specific for each critical subsector, i.e. chemical and energy. Figure 3 on the next page outlines the mapping of these public/private partnerships. This map does not establish any authority besides the President.

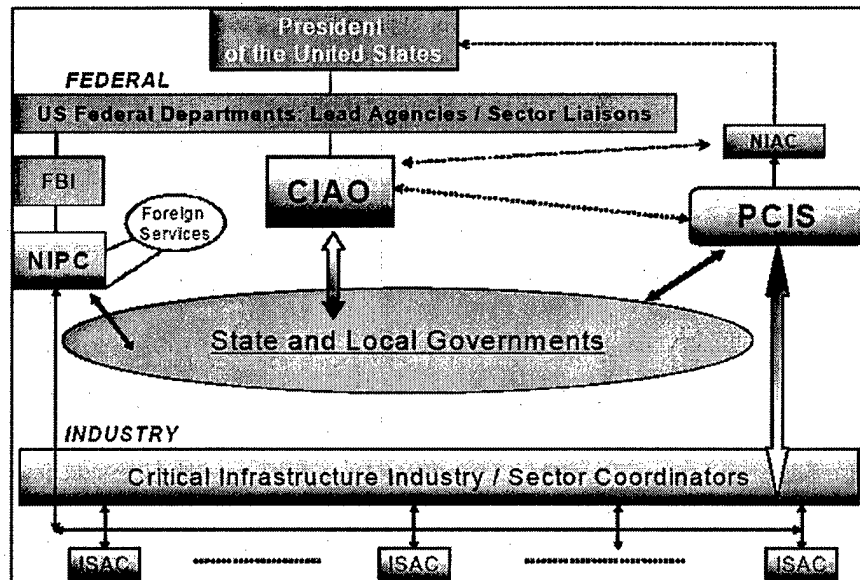


Figure 3: Public-private partnerships in US Critical Infrastructures (Erwann 2003)

2.5. POST 9/11 THREAT RESPONSE

After September 11th, 2001, the United States became much more active in responding to threats. In the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, President Bush outlined several action items for the United States. These items are listed below:

1. Assure public safety, public confidence, and services;
2. Establish responsibility and accountability;
3. Encourage and facilitate partnering among all levels of government and between government and industry;
4. Encourage market solutions wherever possible and compensate for market failure with focused government intervention;
5. Facilitate meaningful information sharing;
6. Foster international cooperation;
7. Develop technologies and expertise to combat terrorist threats; and
8. Safeguard privacy and constitutional freedoms. (Bush 2003)

These eight items serve as the reason for the remainder of the response elements in this section.

2.5.1. Department of Homeland Security

The September 11th attacks resulted in the largest federal reorganization since the formation of the Department of Defense in 1947 (DHS 2003). The Homeland Security Act of 2002 established the Department of Homeland Security and defined its primary missions and responsibilities. The primary missions of the Department include:

- Preventing terrorist attacks within the United States
- Reducing the vulnerability of the United States to terrorism at home
- Minimizing the damage and assisting in the recovery from any attacks that may occur

In order to accomplish its mission and responsibilities, the DHS organized over 170,000 employees into 5 main directorates: Border & Transportation Security, Emergency Preparedness & Response, Science & Technology, Information Analysis & Infrastructure Protection, and Management. The Emergency Preparedness & Response and Information Analysis & Infrastructure Protection directorates are responsible for the construction industry (DHS 2003).

To protect the national infrastructure, the DHS continues to receive increasing funding. The fiscal year 2004 budget request for the DHS is \$36.2 billion. This represents a 7.4% increase in funding over 2003 levels, and a 64 percent increase over 2002. One of the budget priorities pertinent to industrial projects is \$829 million to support the Department's ability to analyze and identify

potential threats, assess vulnerabilities, and provide the information from which to organize protective measures. Another \$500 million is devoted to assess the nation's critical infrastructure (e.g., nuclear power plants, water facilities, telecommunications networks, and transportation systems) and to work to ensure that the highest priority vulnerabilities are addressed (DHS 2003).

2.5.2. National Strategy for Homeland Security

In July 2002, President Bush released the first National Strategy for Homeland Security. This document aligns and focuses homeland security functions into six critical mission areas including protecting critical infrastructure. The major initiatives to protect critical infrastructures include:

- Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets
- Enable effective partnership with state and local governments and the private sector
- Develop a national infrastructure protection plan;
- Secure cyberspace
- Harness the best analytic and modeling tools to develop effective protective solutions
- Guard America's critical infrastructure and key assets against "inside" threats
- Partner with the international community to protect transnational infrastructure. (Bush 2002)

2.5.3. Physical Protection of Critical Infrastructure and Key Assets

In February 2003, President Bush signed the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets to expand on the national strategy outlined in the previous section. This document identifies a clear set of goals and objectives and provides the guiding principles that will underpin the nation's efforts to secure the infrastructures and assets vital to national security (Bush 2003). There are 11 critical infrastructure sectors as identified below in Table 4.

Table 4: Critical Infrastructure Sectors (Bush 2003)

• Agriculture and Food	• Defense Industrial Base
• Water	• Energy
• Public Health	• Transportation
• Emergency Services	• Banking and Finance
• Information and Telecommunications	• Chemical Industry and Hazardous Materials
• Postal and Shipping	

Energy and Chemical/Hazardous Materials are the two main sectors that encompass industrial projects. The strategy outlines security challenges and general initiatives for each of these sectors to accomplish. An example initiative for the Energy sector is to plan and invest in research and development for the oil and gas industry to enhance robustness and reliability (Bush 2003). The National Strategy describes what should be done, but not how to accomplish these objectives.

The document also outlines the government expectations of the private sector. In the present threat environment, the private sector generally remains

the first line of defense for its own facilities. Consequently, private sector owners and operators should reassess and adjust their planning, assurance, and investment programs to better accommodate the increased risks. At the same time though, the federal government will collaborate with the private sector and local governments to provide timely warning and assure the protection of infrastructures and assets that face a specific, imminent threat. The federal government also wants to promote an environment in which the private sector can better carry out its specific protection responsibilities (Bush 2003).

2.5.4. Public/Private Partnerships

According to the National Strategy for Critical Infrastructures and Key Assets, private industry owns and operates approximately 85% of the nation's critical infrastructures and key assets (Bush 2003). Therefore, it is critical to develop a public/private partnership that emphasizes communication flow and shared priorities to secure industrial projects. Information sharing and coordination among private sector and government organizations are essential to thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as recorded in General Accounting Office (GAO) testimony in July 2000, establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult (GAO 2003).

In addition to the Partnership for Critical Infrastructure Security (PCIS), which was established in 1999, another public/private partnership was formed in 2001 called The Infrastructure Security Partnership (TISP). TISP is a group of public and private sector organizations that is an "association of associations and

agencies.” TISP is a partnership, to collaborate on issues related to the security of the nation's built environment. The Construction Industry Institute is one of the founding members of TISP. The fundamental goal of the TISP is to reach and include all stakeholders potentially affected by any disaster and to provide technical assistance and information to the Department of Homeland Security (TISP 2003).

In order to facilitate the partnership process there has been over 50 conferences for infrastructure security. The hosts of these conferences ranged from public agencies, such as the Army Corps of Engineers, to consortiums like the American Society of Civil Engineers (ASCE). The conferences gathered industry professionals to stimulate and share ideas. Unfortunately, the conferences outlined recommendations but did not give any roadmap or tools of how to increase security on industrial projects.

2.5.5. Industrial Specific Guidelines

In October 2001, the American Chemistry Council (ACC) published, “Site Security Guidelines for the U.S. Chemical Industry”. The purpose of the guide is to help managers better protect employees, the community, the environment, plant operations, and company information and product. The ACC outlines elements of a security program by suggesting security practices that managers can consider and tailor to their facilities’ particular situations. Another valuable part of the guidelines is their inclusion of sample policy statements for a new security program. Quoting the guidelines, they serve as a tool rather than a standard (ACC 2001).

In April 2003, the American Petroleum Institute (API) along with the National Petroleum and Refiners Association (NPRA) also published their own industry specific guideline titled, "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries." The methodology constitutes one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. The document provides sample checklists and recommended actions that are industry specific (API 2003).

2.6. DEPARTMENT OF DEFENSE RESPONSES TO 9/11

The Department of Defense (DoD) engineering community has been working on many publications related to antiterrorism/force protection. The initial publication in 2002 was UFC 4-010-01 "DoD Minimum Antiterrorism Standards for Buildings." Note that UFC stands for Unified Facilities Criteria. "Unified" means that it is a joint U.S. Army, U.S. Navy, U.S. Air Force, publication, and is required for use throughout DoD. UFC 4-010-01 is an unrestricted publication. There is also a companion document UFC 4-010-10 that provides design basis threats (explosive weights), but is restricted as For Official Use Only.

The intent of these standards is to minimize the possibility of mass casualties in DoD buildings. The standards provide enforceable measures to establish a level of protection against terrorist attacks for all inhabited DoD buildings where no known threat of terrorist activity currently exists. While complete protection against all potential threats for every inhabited building is cost prohibitive, the intent of these standards can be achieved through prudent

planning, design and construction practices. The financial impact of these standards will be significantly less than the economic and intangible costs of a mass casualty event (DoD 2002).

Two publications due to be published at the end of 2003 include, UFC 4-011-01: "Security Engineering: Programming," and UFC 4-011-02: "Security Engineering: Design." They will replace existing Training Manuals (TM) 5-853-1 thru 3. Over the next five years, the DoD expects to publish 15 more Unified Facilities Criteria standards that are listed in Appendix L (Hartman 2003). These standards will provide the military community a thorough set of objectives and guidelines to follow.

2.7. PROJECT LIFECYCLE

A lifecycle is the set of events (i.e. planning, design, operations, decommissioning) that take place throughout the life of a project. The scope of this thesis focuses on the early stages of the project lifecycle, basically Conceptual (Pre-Project) Planning through Startup. These stages are shown on the next page in Figure 4.

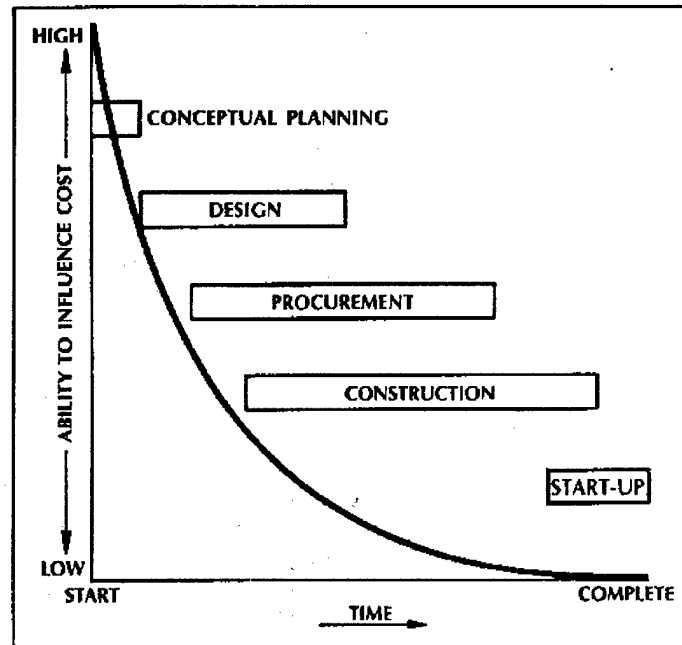


Figure 4: Ability to Influence Final Cost over Project Life (CII 1986)

Figure 4 also shows that maximum benefits occur when people with construction knowledge and experience become involved at the very beginning of a project. There is a large ability to influence cost and project features, such as security. As time continues, the ability to influence is decreased and making adjustments to the project become much more costly.

2.8. SUMMARY

On a monthly basis, more and more documents are published pertaining to security of industrial projects. The government, through the Department of Homeland Security, is becoming very involved with infrastructure security and is working towards developing standards. Public/Private partnerships are being developed with conferences that emphasize information sharing. However, from the literature review conducted, there still seems to be a void in terms of specific

actions for new or retrofit industrial projects. There continues to be an emphasis on “what” should be done rather than “how” to secure a project. The NIST funded study that is outlined in the remaining sections is unique in that will show “how” to address security in the early stages of the industrial project lifecycle.

Chapter 3: Research Methodology

This chapter documents the methodology used to develop the security best practices. It also explains the process by which the author gathered information for this thesis.

3.1. CII/NIST STUDY OVERVIEW

In January 2003, the National Institute of Standards and Technology funded a study in which CII was to determine best practices for project security on industrial projects. In order to accomplish this task, a Steering team and Practice Development team were formed. The Steering team (Appendix A) provided guidance and oversight of the Practice Development team. The Practice Development team (Appendix A) included a facilitator, program manager, corporate security manager, business unit manager, plant operations manager, risk management specialist, and an analyst. The purpose of the Practice Development team was to review, discuss and update existing CII best practices to include security. CII subject matter experts (Appendix A) were also brought in on a case-by-case basis to help with the updates. These different areas of expertise enhanced the review process and ensured that the team maintained a business focus as well as security focus. The author was also a member of the Practice Development team with a primary role to inform the team of any security related events or parallel efforts in other organizations that pertained to security on industrial projects and to support and document this effort.

3.2. SELECTION OF BEST PRACTICES

When the Steering team first formed, the proposed scope of study entailed two or three regional workshops where attendees could gather and discuss evolving practices as companies attempted to improve project security. After further discussion, the Steering team suggested a focus on existing CII best practices. This allowed the team to leverage CII expertise in best practices and use the practice framework as a starting point for a security best practice.

In the March 2003 meeting, the Practice Development team reviewed all the existing and proposed CII best practices. These twenty-six practices have been proven to improve the effectiveness of the project delivery process, but not all are applicable or impacted by security. In order to narrow the selections and find the applicable practices, the Practice Development team used a four-quadrant chart. On the horizontal axis, team members rated the impact of security on the practice from low to high. The vertical axis consisted of a low to high applicability rating of security and the practice. The team came to a consensus on six practices based on a high applicability and high impact towards security. Figures 5 and 6 on the next page summarize the selection process. Figure 5 shows eleven CII Best Practices that have been validated from their benchmarking use, member acceptance or rigorous post research. Figure 6 shows the one additional practice (Planning for Startup) that was selected from the list of proposed best practices. The proposed best practices are just as important as the best practices but they are just pending validation.

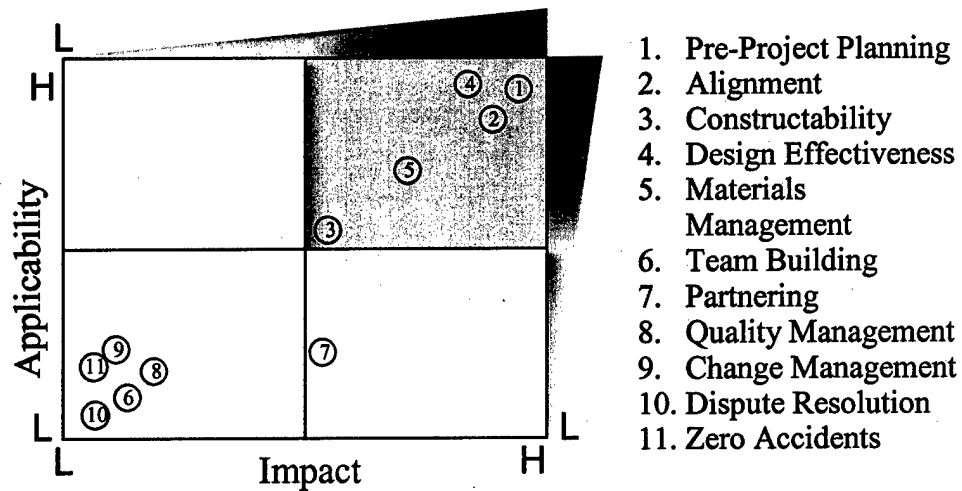


Figure 5: Applicability versus Impact of Best Practices (Sylvie 2003)

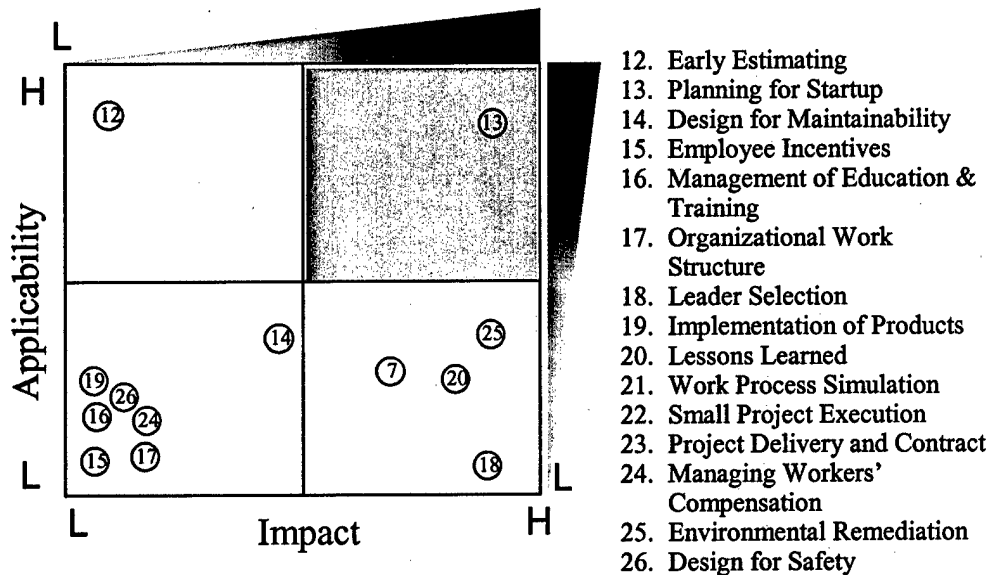


Figure 6: Applicability versus Impact of Proposed Best Practices (Sylvie 2003)

3.3. BEST PRACTICE REVIEW PROCESS

The next stage in the process was to determine the subject matter expert for each practice to assist the team in reviewing the practice. These individuals were selected because they helped the Practice Development team better understand the practice and assisted in identifying security deficiencies. Table 5 lists the subject matter expert for each practice.

Table 5: Subject Matter Experts

Name	Practice(s)	Organization
Gibson, Edd, Ph.D.	Pre-Project Planning (PDRI) & Alignment	University of Texas
Tucker, Richard, Ph.D.	Design Effectiveness	University of Texas
O'Connor, James, Ph.D.	Constructability & Planning for Startup	University of Texas
Bell, Lansford, Ph.D.	Materials Management	Clemson University

3.3.1. Practice Update Example

To illustrate how the best practices were updated, Pre-project Planning will be used as an example. Dr. Edd Gibson is the subject matter expert for Pre-project Planning and he began the meeting by providing the Practice Development team an overview of the practice. With Dr. Gibson there to answer any questions, the team then reviewed the practice manual page by page. Updates to address security during pre-project planning were discussed and inserted only when relevant. The team focused on enhancing the manual to include security, but not rewriting it. After the meeting, CII staff updated the electronic version of the manual to include these security additions. The Practice Development team met the following month to review the changes with

Dr. Gibson and finalized the updates. The end product was an updated CII best practice to show how to properly address security during the front-end planning phase of industrial projects. This same process took place with the other subject matter experts and practices.

Midway through the review process, the Practice Development team determined that a gap existed where CII best practices did not adequately address activities in the construction phase. The Practice Development team then formed a sub-team and developed Job Site Security Guidelines to eliminate the gap. The Job Site Security Guidelines are found in Appendix J. The development of these guidelines rounded out the selection and updating of best practices.

3.3.2. Process Flow Chart

The process flow chart in Figure 7 outlines the process for developing security best practices. Each white item in the flow chart was described in the previous sections. Since the study is broken into two main phases, the bottom part of the chart represents Phase 2 and is shaded gray. This phase of the research effort entails developing a security questionnaire that will be used to populate a database and is not covered in this thesis. The data will eventually allow the impacts of security to be assessed against other project characteristics.

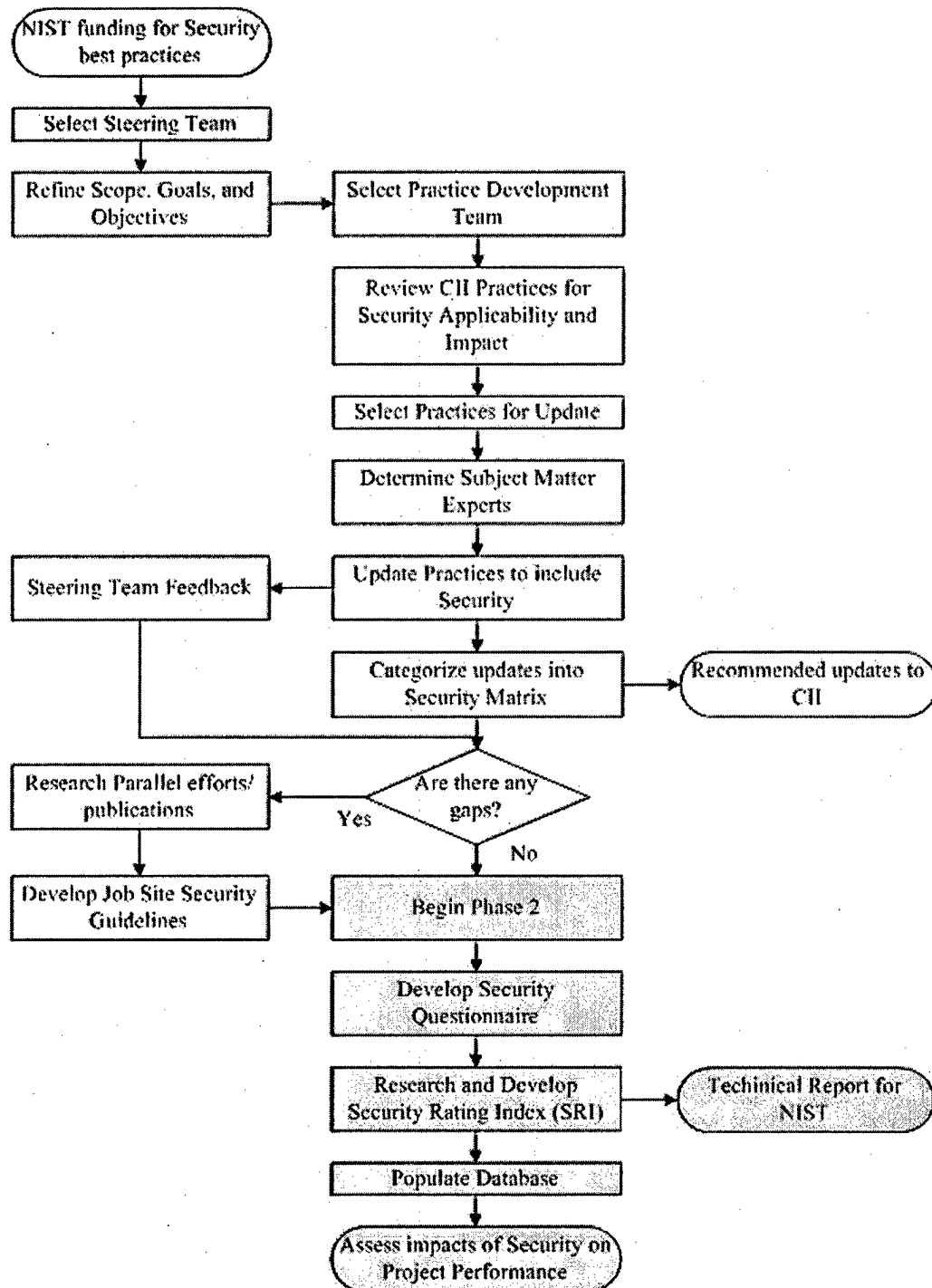


Figure 7: Process Flow Chart for Developing Security Best Practices

Chapter 4: Security Updates

The following chapter describes the major security updates to the CII best practices and their implications to project delivery process.

4.1. PRE-PROJECT PLANNING

4.1.1. Practice Overview

Pre-project Planning is the essential process of developing sufficient strategic information with which owners can address risk and make decisions to commit resources in order to maximize the potential for a successful project. Pre-project Planning is also known as front-end loading, front end planning, and includes feasibility analysis, conceptual planning, programming/schematic design, and early project planning. Greater pre-project planning efforts lead to improved performance on industrial projects in the areas of cost, schedule, and operational characteristics, such as security (CII 2002).

The Project Definition Rating Index (PDRI) for Industrial Projects is a powerful and simple tool used during front-end planning that offers a method to measure project scope definition for completeness. The PDRI offers a comprehensive checklist of 70 scope definition elements in an easy-to-use score sheet format. The PDRI score sheet is supported by detailed descriptions of these elements. An individual, or team, can therefore evaluate the status of their project definition effort during front-end planning and determine their score, or level of definition. Furthermore, since the PDRI element score relates to its risk, high risk areas that need further work can easily be isolated (CII 1996).

4.1.2. Implications of Pre-Project Planning to the Project Delivery Process and Security

Previous CII research shows that effective front-end planning improves project performance in terms of both cost and schedule. The majority of industry participants recognize the importance of scope definition during pre-project planning and its potential impact on project success.

In addition to cost and schedule savings, security will also be enhanced when it is better addressed in front-end planning. Over half of the PDRI elements were updated to include security considerations. Pre-project Planning provides the first opportunity in the project lifecycle to address security. When the project team establishes project objectives of reliability, affordability, feasibility and future expansion, security must also be considered. In fact, security can be an objective of its own in some projects.

Front-end planning is also the time to begin developing specifications and requirements, which should include security considerations. Whether it is the general Civil/Structural/Architectural requirements or specific equipment specifications, incorporating security early in the project lifecycle will cost less than installing a retrofit later on. Security should also be a factor in site selection as well as in technology and process selection.

Document control is important throughout front-end planning. Drawings, correspondence and online documents that slip into the wrong hands could be very detrimental to the security of the project. Front-end planning is also the best time to begin addressing personnel security. This includes proper security education and training as well as clearance for future personnel.

In summary, the elements described above could be addressed later in the project lifecycle but they will be much more costly to incorporate at that point. Industrial projects are very complex, therefore integrating security early on will help increase the security of the project as it becomes operational. Figure 8 shows a cost versus influence curve that is applicable for security. Early in the project, the ability to economically influence security is the highest. As the project proceeds, it becomes more expensive to influence security and the costs for security upgrades increase exponentially.

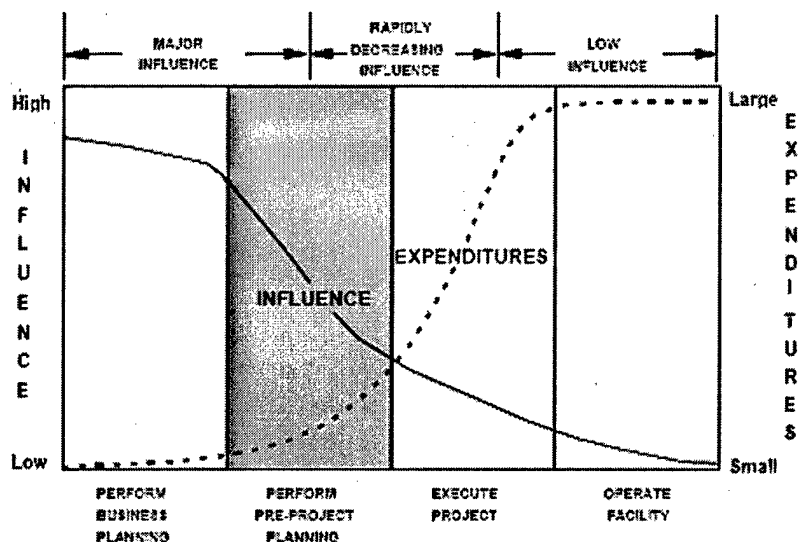


Figure 8: Cost vs. Influence curves for the Project Lifecycle (CII 1996)

4.1.3. Update to Pre-Project Planning Handbook

The Practice Development team reviewed the Pre-project Planning Handbook to identify areas where security should be added. The team added

security to the manual as shown in Figure 9. The complete list of updates is found in Appendix C.

Page 3 changes

When the pre-project planning effort is finished, one should have completed the following to ensure a high level of confidence in the success of the project:

- *addressed business requirements for the project*
- *selected critical technologies for the project*
- *addressed security issues and conducted vulnerability assessment*

Page 26 changes

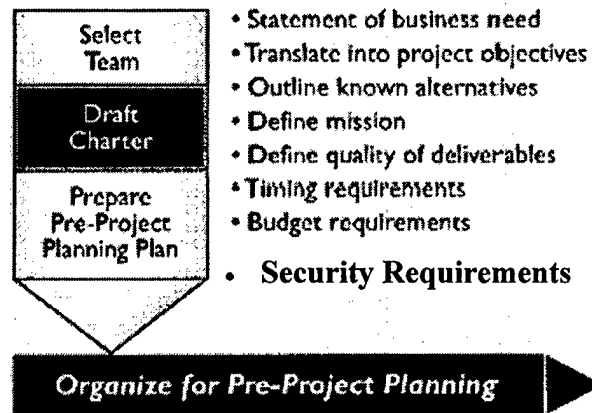


Figure 9: Example updates to Pre-Project Planning Handbook (changes in bold)

4.1.4. Update to PDRI

The Practice Development team reviewed the 70 elements of the PDRI for Industrial projects to identify areas where security could be added. The team recommended updates for 37 of the 70 definitions. These updates may not change the scoring of the PDRI, but they do enhance the supporting definitions.

Two example updates are shown below in Figure 10 with the changes indicated in bold. The complete list of updates is found in Appendix D.

D. PROJECT SCOPE

D1. Project Objectives Statement

This is a mission statement that defines the project objectives, **including security considerations**, and priorities for meeting the business objectives. It is important to obtain total agreement from the entire project team regarding these objectives and priorities to ensure alignment.

H. EQUIPMENT SCOPE

H1. Equipment Status

Has the equipment been defined, inquired, bid tabbed, or purchased?
This includes all engineered equipment such as:

- ☐ Process
- ☐ Electrical
- ☐ Mechanical
- ☐ HVAC
- ☐ Instruments
- ☐ **Security-related equipment**
- ☐ Specialty items
- ☐ Distributed control systems

Figure 10: Example updates to PDRI Elements (changes in bold)

4.2. ALIGNMENT

4.2.1. Practice Overview

As defined in IR 113-3, alignment is the condition where appropriate project participants are working within acceptable tolerances to develop and meet a uniformly defined and understood set of project objectives. Figure 11 shows that alignment must take place throughout the project lifecycle.

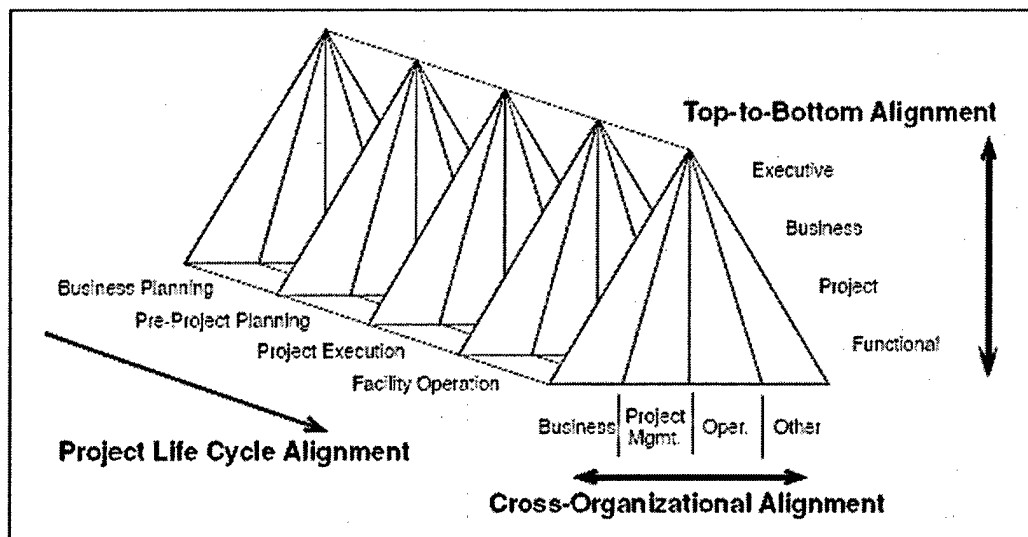


Figure 11: 3-D Schematic Organizational Alignment for a Project (CII 1997)

There are ten critical alignment issues that have the greatest effect on front-end planning. When project teams focus on these issues, alignment improves and the likelihood of a successful project greatly increases. The issues are:

1. Stakeholders are appropriately represented on the project team.
2. Project leadership is defined, effective, and accountable.

3. The relative priorities among cost, schedule, safety, and required project features are clear.
4. Communication within the team and with stakeholders is open and effective.
5. Team meetings are timely and productive.
6. The team culture fosters trust, honesty, and shared values.
7. The pre-project planning process includes sufficient funding, schedule, and scope to meet the project objectives.
8. The reward and recognition system promotes meeting or exceeding the project objectives.
9. The teamwork and team building programs are effective.
10. Planning tools (e.g., checklist, simulations, and work flow diagrams) are effectively utilized (CII 1997).

4.2.2. Implications of Alignment to the Project Delivery Process and Security

Alignment is a very important issue in the security of industrial projects. The first alignment issue that the Practice Development team updated was stakeholder representation the project team (Issue #1 of the 10 critical alignment issues in the previous section). For security, a dedicated security manager needs to be a member of the project team. The security manager is responsible for screening personnel, suppliers, and ensuring security is covered throughout the project lifecycle.

Secondly, the team needs to be aligned with the priorities between cost, schedule and specific project features like security (Issue #3). Depending on the vulnerability assessment, some projects must consider security features more than others. The team must emphasize alignment throughout the project delivery process and especially when the project exceeds the budget or schedule. Understanding the balance of priorities requires the third item, which is open and effective communication (Issue #4). Since the early planning phase of a project

is characterized by many decisions that will significantly affect the entire project, each stakeholder should have a voice in the project delivery process to be successful.

Finally, the overall pre-project planning process must be structured and resourced (Issue #7). If security is one of the key project objectives, the team must devote sufficient funding, schedule and scope to meet that objective. Alignment must be maintained throughout the project delivery process.

4.2.3. Update to Alignment

As mentioned in the previous section, the Practice Development team made security updates to 4 out of 10 critical alignment issues. These issues were

- Stakeholders are appropriately represented on the project team.
- The relative priorities among cost, schedule, safety, and required project features are clear.
- Communication within the team and with stakeholders is open and effective.
- The pre-project planning process includes sufficient funding, schedule, and scope to meet the project objectives.

The Practice Development team made other updates to CII Implementation Resource 113-3 when security was important. Two example updates are identified on the next page in Figure 12. The full list of updates is found in Appendix E.

Page 22 changes

Key Execution Process Issue #1: Stakeholders are appropriately represented on the project team.

The pre-project planning team should include representatives from all significant project stakeholders. Stakeholders are defined as those directly or indirectly associated with the project, those affected by the project and its activities, and those interested in the outcome of the project. The team needs to include representatives from operations, construction, business management, **security**, and other stakeholder groups as well as project management and engineering, **as appropriate**. Those projects involving joint ventures, complex internal business organizations, or outside consultants should be especially cognizant of this issue.

Page 33 changes

The CII Agreement Matrix is an efficient tool for identifying, prioritizing, communicating, reinforcing, and controlling project objectives. This tool quantifies agreement between various project participants. (CII Publication 12-1, *Setting Project Objectives*, provides a complete description of the development and uses of the Agreement Matrix.) **Security is a priority that must be addressed. By conducting a comprehensive vulnerability assessment during the initial stages, project leaders can determine appropriate security measures required at each stage of project development.**

Figure 12: Example updates to Alignment (changes in bold)

4.3. DESIGN EFFECTIVENESS

4.3.1. Practice Overview

Design effectiveness is an all-encompassing term to measure the results of the design effort, including input variables and design execution, against the specified expectations of the owner (CII 2002).

Design is perhaps the most central point of definition for a project in that ideas and information are transcribed to paper in the form of specific and coordinated instructions for the project's construction and documentation. Many contributors are involved during the design phase including the owner, the various designer groups, vendors, and construction representatives. As a result, it is difficult then to evaluate the performance of a specific party, but much easier to evaluate the overall results of all parties. Many elements contribute to the design product. In Research Summary (RS) 8-1, the following seven evaluation criteria were determined to be the most significant in the evaluation process:

1. Accuracy of Design Documents
2. Usability of Design Documents
3. Cost of Design
4. Constructability
5. Economy of Design
6. Performance Against Schedule
7. Ease of Startup (CII 1986)

The above criteria do not influence a design to the same degree. An Objectives Matrix is a method of assigning weights and performance ratings into

a single performance index number. The Practice Development team reviewed these seven criteria and determined that security should be added to the Objectives Matrix when it is a project objective. A sample Objective Matrix with security included is found in Appendix F.

4.3.2. Implications of Design Effectiveness to the Project Delivery Process and Security

The security implications of design to the project delivery process were summarized very well by the update on Page 8 of Research Summary 8-1.

Security throughout the project life cycle is directly linked to the effectiveness of the design effort. A quality design considers this element throughout the project. Security considerations are derived from the vulnerability assessment. An effective design will help decrease associated security vulnerabilities.

The design effort must address security, as appropriate, to be effective. During the design phase the plot plan and permitting plan are being finalized. The project team is also designing security features for the operational facility. These elements are critical to the physical and information security of the project. A distribution matrix is also important during the design phase to ensure document control. Documents such as CAD drawings and project correspondence could be detrimental to the project if they are in the wrong hands. If the vulnerability assessment determines the importance of security, this criteria needs to be added to the Objective Matrix to evaluate design.

4.3.3. Update to Design Effectiveness

As mentioned in the previous section, the Practice Development team updated RS 8-1, to highlight security as a potential project objective and design

evaluation criteria. Two updates are identified in Figure 13 with the changes indicated in bold. The full list of updates is found in Appendix F.

Page 5 changes

4: DESIGN EVALUATION CRITERIA

These seven criteria are not all-inclusive for measuring design effectiveness. **If the Vulnerability Assessment indicates that security is an essential element of the project, add Security as a criterion in the Objective Matrix.** Other criteria relating to operability, maintainability, safety, plant operating efficiency, and plant performance are at least of equal importance. These latter criteria, however, require evaluations after a period of plant operation and by different personnel than those involved in a project's design, construction, and start-up. Thus, they are not included in this publication. The seven criteria included in Figure 1 can be evaluated before the project team disperses and important data become unavailable.

CRITERIA	Quantitative	Subjective
Accuracy of Design Documents	X	
Usability of Design Documents		X
Cost of Design Effort	X	
Constructability of Design		X
Economy of Design		X
Performance Against Schedule	X	
Ease of Start-Up	X	
Security	X	

Figure 13: Example updates to Design Effectiveness (changes in bold)

4.4. CONSTRUCTABILITY

4.4.1. Practice Overview

Constructability is the effective and timely integration of construction knowledge into the conceptual planning, design, construction and field operations of a project to achieve the overall project objectives in the best possible time and accuracy at the most cost-effective levels (CII 2002). There are 17 main constructability concepts identified in Implementation Guide 34-1.

4.4.2. Implications of Constructability to the Project Delivery Process and Security

Many of the benefits of constructability are identified in IR 166-3. Previous research shows that constructability reduces overall project costs 4.3 percent and reduces project schedule 7.5 percent on average. Constructability increases project quality in terms of operability, functionality, and reliability. Finally, constructability also enhances the progress of the work, i.e. planning, design, construction, and startup schedules (CII 2002).

Security is also related to constructability throughout the project delivery process. The Engineering/Construction plan must consider the tradeoffs between constructability and security. A site that is very secure might be difficult to construct and vice versa. However, it is possible to increase both security and constructability. For example, modularization allows for major off site construction in a secure facility. Once the elements are on site, they are rapidly assembled and potentially decrease the physical, personnel and

information vulnerabilities to industrial projects. At the same time though, modularization can create security risks if there is a lack of control off-site.

4.4.3. Update to Constructability

The Practice Development team reviewed Implementation Guide 34-1 for security updates. In addition to updates throughout the introductory material, the team found that 12 of the 17 constructability concepts in Tool 17 were applicable towards security. Tool 17 is the best tool to summarize the constructability concepts presented in 34-1. The twelve concepts that are applicable towards security are identified with a star (*) in Table 6:

Table 6: Constructability Concepts (CII 1993)

Concept	Concept Name
* I-1	Constructability program is an integral part of project execution plan.
* I-2	Project planning involves construction knowledge.
I-3	Early construction involvement is considered in development of contracting strategy.
* I-4	Project schedules are construction sensitive.
* I-5	Site layouts promote efficient construction.
* I-6	Basic design approaches.
* I-7	Project team participants responsible for constructability are identified early on.
* I-8	Advanced information technologies are applied throughout project.
II-1	Design and procurement schedules are construction sensitive.
* II-2	Designs are configured to enable sufficient construction.
II-3	Design elements are standardized.
* II-4	Construction efficiency is considered in specification development.
* II-5	Module/preassembly designs are prepared to facilitate fabrication, transport, and installation.
* II-6	Designs promote construction accessibility of personnel, material, and equipment.
* II-7	Designs facilitate construction under adverse weather conditions.
II-8	Design and construction sequencing should facilitate system turnover and start-up.
III-1	Constructability is enhanced when innovative methods are utilized.

Two example updates in the introductory material of Implementation Guide 34-1 are identified in Figure 14 with changes indicated in bold. The remaining updates are found in Appendix F.

Page 22 changes

The intangible benefits from constructability are as important as the quantitative benefits, and must be recognized accordingly. These include more accurate budgets and schedules, improved site layouts, improved project team relationships, more repeat work, **improved security**, and many others.

Page 37 changes

Establish constructability objectives. Once the design and construction participants are involved, a specific set of constructability objectives can be developed. This set of objectives can be used to enable trade-off analysis between constructability and other project considerations, **such as security**.

Figure 14: Example updates to Constructability (changes in bold)

4.5. MATERIALS MANAGEMENT

4.5.1. Practice Overview

Materials management is an integrated process for planning and controlling all necessary efforts to make certain that the quality and quantity of materials and equipment are appropriately specified in a timely manner, are obtained at a reasonable cost, and are available when needed. The materials management systems combine and integrate the takeoff, vendor evaluation, purchasing, expediting, warehousing, distribution, and disposing of materials functions (CII 2002).

The cost of materials represents more than half of the total cost of today's typical project. Lack of materials when needed at the job site can cause

expensive construction delays. Given the impact on cost and schedule, it is easy to see the positive influence that effective materials management can have on the cost of construction. CII research indicates that adequate planning may be the single most important determinant of effective project materials management and materials management is the most important practice for schedule performance (CII 1999).

4.5.2. Implications of Materials Management to the Project Delivery Process and Security

Management of materials is critical to security in the project delivery process. Planning for material management is the first important step. The project team needs to have plans and procedures for warehousing, inventory control and the overall delivery process. At the same time, the security manager must ensure the proper execution of these plans by including them as part of the overall project security plan.

Developing partnerships and alliances with suppliers will also increase security. Partnerships and alliances are critical to materials management, but also important to all the other phases of the project lifecycle. All suppliers and delivery personnel should still be screened prior to selection. Even though there may be a partnership, the project team should also only share "need to know" information with the supplier.

Materials management in industrial projects often involves hazardous or security sensitive materials. The project team needs to ensure these materials are secure when they are transported and while on site. Security vulnerabilities are decreased if the materials arrive "just in time." Security related equipment must

also be properly defined and purchased during the procurement phase. Most importantly, the equipment must be purchased with appropriate input from the security manager and operations and maintenance manager if possible.

4.5.3. Update to Materials Management

The Practice Development team reviewed Implementation Resource 7-3 for possible security additions. Two example updates are identified in Figure 15 with team changes identified in bold. The remaining updates are found in Appendix H.

Page 2-10 changes

There are other factors that may contribute to the analysis and decision for extensive prefabrication including:

- Equipment
- Safety
- **Security**
- Schedule

Page 6-22 changes

4.8.4 Logistics Strategy

Consideration of transportation capabilities to, from, and on-site, including duration, equipment availability, **security requirements**, facilities, traffic control, expediting and cost.

Figure 15: Example updates to Materials Management (changes in bold)

4.6. JOB SITE SECURITY

4.6.1. Practice Overview

Job site security is not a CII best practice but it is covered here before Planning for Startup because of its timing and importance in the project lifecycle. The procedures for job site security were developed on a conceptual level by a sub-team to the Practice Development team. Sub-team members included two security professionals, a facilitator and an analyst. The need for job site security guidelines was first identified through a gap analysis of the project lifecycle. The six best practices selected for updates covered almost every aspect of the project from pre-project planning through startup. The one area that was not covered explicitly was security on the job site during the construction phase. The job site security guidelines identified by the sub-team successfully fill this gap.

4.6.2. Implications of Job Site Security to the Project Delivery Process and Security

Job site security is very important to the industrial project delivery process. First of all, the job site may need a dedicated security coordinator depending on the size and scope of the project. This coordinator is responsible for developing and implementing a construction site security plan. Some features of this plan include proper access control procedures as well as measures to ensure the perimeter is monitored. If there are any security breaches or incidents, follow up must occur to determine why the event happened necessary action must be taken. The security coordinator should also meet with local

authorities to develop emergency response plans for the site. Job site personnel need to be trained to identify suspicious activities and take appropriate actions. The culmination of the actions identified above is a job site that is secure and does not create any unwanted vulnerabilities to the operational facility.

4.6.3. Update to Job Site Security

The full text of the Job Site Security Guidelines is found in Appendix I. Two samples of the guidelines are found in Figure 16.

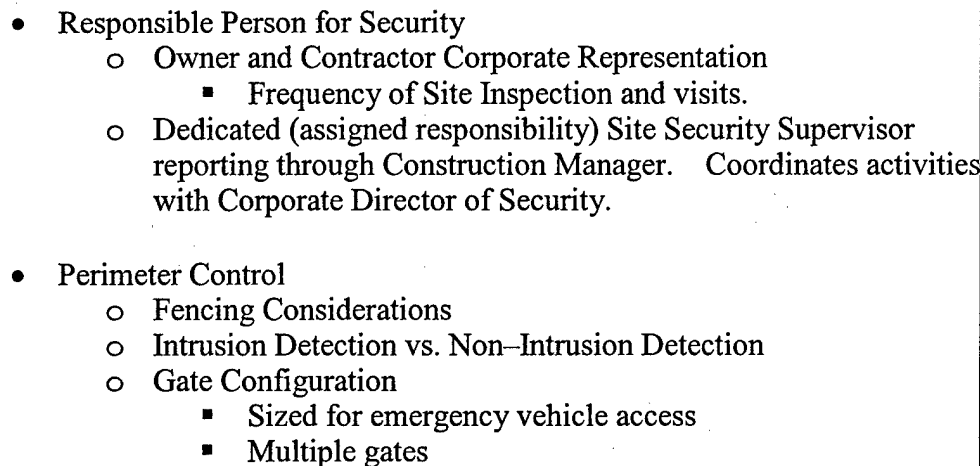
- 
- Responsible Person for Security
 - Owner and Contractor Corporate Representation
 - Frequency of Site Inspection and visits.
 - Dedicated (assigned responsibility) Site Security Supervisor reporting through Construction Manager. Coordinates activities with Corporate Director of Security.
 - Perimeter Control
 - Fencing Considerations
 - Intrusion Detection vs. Non-Intrusion Detection
 - Gate Configuration
 - Sized for emergency vehicle access
 - Multiple gates

Figure 16: Example updates to Job Site Security Guidelines

4.7. PLANNING FOR STARTUP

4.7.1. Practice Overview

Plant startup is defined as the transitional phase between plant construction completion and commercial operations, including all of the activities that bridge these two phases. Critical steps within the startup phase include

system turnover, checkout of systems, commissioning of systems, introduction of feedstocks, and performance testing (CII 1998).

Startup is a critical phase in the project lifecycle and must be given adequate attention. Implementation Resource 121-2 identifies the Startup Planning Model to help industry plan startups in a more thorough, effective, and efficient manner. The Startup Planning Model is a sequence of 45 planning activities organized according to eight project phases (see Table 7 below).

Table 7: Startup Planning Model Phases and Activities (CII 1998)

Project Phase	No. of Startup Planning Activities
Requirements Definition and Technology Transfer	1
Conceptual Development and Feasibility	3
Front-End Engineering	10
Detailed Design	15
Procurement	3
Construction	7
Checkout & Commissioning	3
Initial Operations	3

4.7.2. Implications of Planning for Startup to the Project Delivery Process and Security

Even though startup is the final phase of the project delivery process, there are still many security risks. However, proper startup planning throughout the earlier stages allows for a smooth, more secure startup. The project team needs to set requirements and objectives for startup pre-commissioning and turnover sequences. Training plans for the proper use of equipment and information systems are also implemented during startup. Operations and Maintenance

personnel should be screened during the startup phase. Also, the project team needs to determine the security effects from construction change orders and make any necessary last minute adjustments prior to the facility being operational. The actions mentioned above should all be a part of the Startup Security Plan that is now added to IR 121-2. Startup security is an ongoing process that must be planned for early in the lifecycle in order to decrease project vulnerability.

4.7.3. Update to Planning for Startup

The Practice Development team reviewed the 45 planning activities in IR 121-2 and made updates as necessary to address security. The team also identified three new activities to Plan for Startup Security (Activity 3-X), Update the Startup Security Plan (Activity 4-X), and Finalize the Startup Security Plan (Activity 6-X). These activities have an "X" because they are new and need a placeholder in the manual. Two sample updates are identified on the next page in Figure 17 with changes indicated in bold. The complete list of updates, including the new activities, is found in Appendix J.

Page 31 changes

3-A: Establish Startup Objectives

I. Challenges to Successful Implementation:

- Lack of understanding of startup objectives and their importance on the part of the business unit.
- Misalignment of startup objectives between project management and business unit personnel.
- **Security is sometimes overlooked as a startup objective.**

Page 82 changes

4-C: Plan for Supplier Field Support of Startup

G. Basic Steps:

1. Understand and commit to the requirements of the existing change management system (thoroughly establish one if none exists!).
2. Add assessment of startup impacts to the change evaluation system, and whenever appropriate, involve startup expertise in the change management team.
3. Recognize that changes can cause delays, cost increases, unforeseen safety and health risks, **new security challenges**, loss of momentum, demotivated workers, and loss of organization and planning.

Figure 17: Example updates to Planning for Startup (changes in bold)

4.8. SUMMARY

This chapter described how the Practice Development team updated six CII best practices and their implications to the capital facility delivery process and security. In order to summarize the concepts of these updates, the Practice Development team organized the information in a matrix. Figure 18 is an

example of a portion of the Security Matrix that the team developed. Updates were organized by project phase and type of security (Physical, Personnel, and Information) with the understanding that some updates fit in more than one phase. Figure 18 shows the updates for Front End Planning (FEP). The Security Matrix allowed the team to analyze the project by phase and determine if additional gaps existed. The complete Security Matrix is found in Appendix K.

Phase	Physical	Personnel	Information
FEP	Security Stakeholders on P3 Team (AI #1)	Social Issues (B8)	CADD/Model Requirements (M1)
	Reliability Philosophy (A1)		
	Operating Philosophy (A3)	Training Requirements for Operational Facility (P6)	Document Control Systems (M3)
	Affordability/Feasibility (B4)		
	Process Simplification (E1) <i>and so on...</i>		

Figure 18: Security Matrix example

Chapter 5: Conclusions and Recommendations

5.1. CONCLUSIONS

Project and facility security have become very important since the attacks of September 11th, 2001. As a result, the National Institute of Standards and Technology (NIST) funded a study for the Construction Industry Institute (CII) to develop best practices for industrial project security. This thesis summarizes the results of the research effort. The objectives of this thesis were to:

1. Summarize homeland security literature as it pertains to industrial projects
2. Determine and adapt applicable CII best practices to develop a security best practice
3. Provide recommendations for industry implementation

Chapter 2 focused on accomplishing the first objective. Definitions of Security, Threat and Consequences were provided as well as the overview of the Security Vulnerability Assessment. There was a review of historical industrial terrorism events in Bhopal, and the Kuwait refinery fires. Industry threats were outlined as well as responses to those threats. Since September 11th, 2001, many organizations have mobilized to try to increase security in industrial projects. However, there has been an emphasis on “what” to do for project security rather than “how” to do it. The “how” is answered with Objective 2.

Objective 2 focused on determining which CII practices were applicable towards industrial project security and adapting them to develop a security best practice. Chapter 3 outlines how the Practice Development team reviewed all

existing and proposed CII best practices for their applicability and impact with respect to security. The team selected six best practices, and after a gap analysis, developed the job site security guidelines. These seven elements cover the early stages of the project lifecycle from Front End Planning through Startup. Once the applicable practices were determined, the Practice Development team made updates to each one in order to satisfy the second objective.

Chapter 4 highlighted the process of adapting the best practices by providing a brief overview of the practice, sample updates and the implications toward the project delivery process. The full list of updates is found in Appendices C through H. The depth of these updates shows how thoroughly the team reviewed the documents and made security updates where applicable. At the same time, the team focused on not changing any of the original process that made each practice a “Best Practice.” The result is a set of recommended updates that show “how” a project team can move through the project lifecycle and adequately address security at each stage.

Objective 3 is answered in the next section with a list of recommendations to industry, CII and the U.S. Air Force.

5.2. RECOMMENDATIONS

5.2.1. Recommendations to Industry

Industrial projects are very complex and project teams have to focus on many issues. The mindset of cost, schedule, and quality needs to be expanded to look at other project features like security. The industry as a whole should work towards a culture that promotes a better security mindset.

Standards and guidelines have been developed to a small extent but more unified efforts are still needed. A common definition of who sets policy and what level of authority they possess is also required. Eventually, there should be uniformity of codes across Federal, State, and Local levels. These codes will serve as a part of the baseline design. Industry involvement in the development of codes and standardization of procedures is vital.

Technology is the final area that must be addressed. In today's environment, technology is constantly changing and advancing. Industrial members should keep an eye on other industries to see what is being developed and if they can use these advancements. Some examples of areas that could benefit from technology development include: the specification and loading of materials to assure security of contents, new technology to protect process control systems, and technology for physical security and resiliency of facilities. The industry should also work on developing systems that mitigate threats as they are discovered or received.

5.2.2. Recommendations to CII

The Construction Industry Institute should follow through with the recommended updates provided by the Practice Development team. This will officially update the six best practices in terms of security. Eventually, CII should work towards developing a stand-alone security practice. This would include a means to rate security at multiple stages in the project lifecycle through the use of a questionnaire. A questionnaire that is used across the industry could serve as a method to help with standardization of procedures. This study

focused on industrial projects. Funding should be made available to research other industry groups such as buildings. Finally, security should be added to the benchmarking database in order to analyze tradeoffs with other features such as cost, schedule and safety.

5.2.3. Recommendations to United States Air Force

Basically, all of the recommendations for industry also apply to the U.S. Air Force. In addition to those outlined in Section 6.1, the following actions are recommended.

Recent terrorism events have changed the military's base defense strategies. Currently, security is considered an "additional duty" for a young officer or senior non-commissioned officer. In order to properly respond and prepare for future attacks, the U.S. Air Force should create a sub-unit or "flight" within Civil Engineering that focuses on security. This unit needs a separate funding source and the ability to focus solely security responsibilities. Since the U.S. Air Force rotates personnel every two to three years, a dedicated unit helps the continuity of information and objectives. It also eliminates the learning curve that currently exists for learning the additional duty. A security flight facilitates better communication of security objectives with contractors, which is critical seeing that the majority of military construction is now performed via contract. A security sub-unit with expertise will eventually save the U.S. Air Force money because proper security planning on construction projects will eliminate the need for expensive retrofits.

Although this thesis focuses on industrial projects, the construction management principles presented are also beneficial to the U.S. Air Force. The practices presented by CII (e.g. Pre-project Planning and Materials Management among others), have been shown to increase project success. The U.S. Air Force should consider renewing its membership in CII and be more active in benchmarking their projects. The U.S. Air Force should also use the security concepts presented in this thesis for any new or retrofit construction project.

Appendix A: Committee Membership

Steering Team membership:

Name	Position	Company
Dunn, Stretch	Director of Federal Programs	BE&K (Retired)
Poer, Charles	Business Unit Manager	Zachry
Porter, Jim	Vice President	DuPont
Syphard, David	Vice President	Jacobs
Chapman, Bob	Economist	NIST
McGinnis, Chuck	Facilitator	CII (Retired)
Thomas, Steve	Associate Director	CII

Practice Development Team membership:

Name	Function	Company
McGinnis, Chuck	Facilitator	CII (Retired)
Toadvine, Jay	Program Manager	Fluor
Spight, Michael	Corp. Security Manager	Black & Veatch/TRC Companies
Brady, John	Corp. Security Manager	ConocoPhillips
Lisiewski, Walter	Business Unit Manager	Jacobs
Hewitt, Michael	Plant Operation Manager	DuPont
Staton, Gary	Risk Management Specialist	DuPont
Lee, Shawn	Analyst	CII
Snyder, Roger	Ex-Officio (CII Education Comm.)	U.S. Dept. of Energy
Chapman, Bob	Ex-Officio / Sponsor	NIST
Thomas, Steve	Ex-Officio / Principal Investigator	CII
Sylvie, Jon	Ex-Officio / Graduate Res. Assist.	U.T. Austin
Matthews, Ben	Ex-Officio / Graduate Res. Assist.	U.T. Austin

Subject Matter Experts:

Name	Practice(s)	Organization
Gibson, Edd, Ph.D.	Pre-Project Planning (PDRI) & Alignment	University of Texas
Tucker, Richard, Ph.D.	Design Effectiveness	University of Texas
O'Connor, James, Ph.D.	Constructability & Planning for Startup	University of Texas
Bell, Lansford, Ph.D.	Materials Management	Clemson University

Appendix B: Practice Development Team Meeting Agendas

March 3-4, 2003

Monday – Mar 3rd

Time	Activity	Location
7:30 - 9:00	PI/NIST/Facilitator Pre Meeting	Room 2.9134
9:00 - 9:15	Team Meeting Begins - Welcome & Introductions	Alamo Room (3.604)
9:15 - 9:30	Study Background by the PI	"
9:30 - 10:00	Overview of CII and CII Resources	"
10:00 - 10:30	NIST/PI Guidance on Final Product	"
10:30 - 10:45	Break	"
10:45 - 11:15	Update & Discussions of the Threat and Parallel Efforts	"
11:15 - 12:00	Review of CII Best Practices	"
12:00 - 12:30	Lunch	"
12:30 - 2:00	Review of CII Best Practices Continues	"
2:00 - 2:15	Break	"
2:15 - 3:00	Select & Prioritize Best Practices for Study	"
3:00 - 3:30	Layout Schedule	"
3:30 - 4:30	Determine Subject Matter Experts	"
4:30 - 5:00	Wrap-up for the Day	"
5:00 -	Meeting Adjourns	"

Tuesday – Mar 4th

Time	Activity	Location
7:30 - 8:00	Continental Breakfast	Alamo Room (3.604)
8:00 - 9:30	Presentation of Pre-Project Planning Best Practice & PDRI by Dr. Edd Gibson	"
9:30 - 9:45	Break	"
9:45 - 12:00	Discussion/Integration of Security Issues	"
12:00 - 12:30	Lunch	"
1:00 - 2:30	Discussion/Integration of Security Issues	"
2:30 - 3:00	Update Schedule & Discuss Plans for Next Meeting	"
3:00	Meeting Adjourns	"

April 3-4, 2003

Thursday – April 3rd

<u>Time</u>	<u>Activity</u>	<u>Location</u>
9:00 - 9:10	Welcome & Announcements	Mt. Bonnell 3.602
9:10 - 9:30	New Team Member Orientation	“
9:30 - 10:30	Review of PDRI Product	“
10:30 - 10:45	Break	“
10:45 - 12:00	Continue PDRI Product Review	“
12:00 - 1:00	Lunch	
1:00 - 1:30	Threat Update & Parallel Developments	“
1:30 - 3:30	Pre-Project Planning Manual Security Review	“
3:30 - 3:45	Break	
3:45 - 4:45	Methodology Review	“
4:45 - 5:00	Questions, Announcements, Adjournment	“

Friday – April 4th

<u>Time</u>	<u>Activity</u>	<u>Location</u>
7:30 - 8:00	Continental Breakfast	Mt. Bonnell 3.602
8:00 - 9:00	Alignment Best Practice Briefing	“
9:00 - 10:15	Integration of Security Issues (Alignment)	“
10:15 - 10:30	Break	
10:30 - 12:00	Design Effectiveness Best Practice Briefing	“
12:00 - 1:00	Lunch	
1:00 - 2:45	Integration of Security Issues (Design Effectiveness)	“
2:45 - 3:00	Future Meeting Plan, Announcements, Adjournment	“

May 15-16, 2003

Thursday – May 15th

<u>Time</u>	<u>Activity</u>	<u>Location</u>
9:00 - 9:10	Welcome & Announcements	Barton Springs Room 1.304
9:10 - 10:00	Review of Alignment IR113-3 Changes	“
10:00 - 10:30	Review of Design Effectiveness Pub 8-1	“
10:30 - 10:45	Break	“
10:45 - 12:00	Review of Pre-Project Planning Handbook	“
12:00 - 1:00	Lunch	
1:00 - 2:00	Threat Update & Parallel Developments	“
2:00 - 3:00	Meaning of the Security Rating Index	“
3:00 - 3:15	Break	
3:15 - 4:45	Review of Chemical Industry Site Security Guidelines	“
4:45 - 5:00	Questions, Announcements, Adjournment	“

Friday – May 16th

<u>Time</u>	<u>Activity</u>	<u>Location</u>
7:30 - 8:00	Continental Breakfast	Barton Springs Room 1.304
8:00 - 9:00	Constructability Best Practice Presentation/Discussion	“
9:00 - 10:15	Integration of Security Issues (Constructability)	“
10:15 - 10:30	Break	
10:30 - 11:00	Planning for Start-Up Best Practice Presentation/Discussion	“
11:00 - 12:00	Integration of Security Issues (Planning for Start-Up)	“

12:00	-	12:45	Lunch	
12:45	-		Value Management Processes Discussion	“
		2:45		
	-		Future Meeting Plan, Announcements,	“
2:45		3:00	Adjournment	

June 18-19, 2003

Wednesday – June 18th

<u>Time</u>	<u>Activity</u>	<u>Location</u>
9:00 - 9:10	Welcome & Announcements	Mt. Bonnell 3.602
9:10 - 10:00	Review of Construction Site Security Plan	“
10:00 - 11:00	Development of the Security Rating Index	“
11:00 - 11:15	Break	“
11:15 - 12:00	Continue Development of the Security Rating Index	“
12:00 - 1:00	Lunch	“
1:00 - 2:30	Methodology for Use of the Security Rating Index	“
2:30 - 2:45	Break	“
2:45 - 3:15	Threat Update & Parallel Developments	“
3:15 - 3:45	Review of Constructability 34-1 Changes	“
3:45 - 4:45	Review of Planning for Startup IR121-1 Changes	“
4:45 - 5:00	Questions, Announcements, Adjournment	“

Thursday – June 19th

<u>Time</u>	<u>Activity</u>	<u>Location</u>
- 8:00	Continental Breakfast	Mt. Bonnell 3.602
7:30 - 9:30	Materials Management Best Practice Presentation & Discussion	“
8:00 - 10:30	Presentation & Review of IR 7-3 Procurement and Materials Management	“
10:30 - 10:45	Break	“
10:45 - 12:00	Integration of Security Issues for Material Management	“
12:00 - 1:00	Lunch	“
1:00 - 2:00	Integration of Security Issues for Material Management Continued	“
2:00 - 2:15	Break	“
2:15 - 2:45	Presentation Plan for Annual Conference	“
-	Future Meeting Plan, Announcements,	“
2:45 - 3:00	Adjournment	

July 15 Conference Call

1. Review Annual Conference slides & program
2. Discuss questionnaire development & scoring algorithm
3. Discuss tool development
4. Review current questionnaire
5. Discuss proposed path forward

Appendix C: Pre-Project Planning Handbook Updates

The following updates were made to CII Special Publication 39-2 "Pre-Project Planning Handbook" (1995). Changes are indicated in bold and begin on page 3 of the publication.

Page 3 changes

When the pre-project planning effort is finished, one should have completed the following to ensure a high level of confidence in the success of the project:

- *addressed business requirements for the project*
- *selected critical technologies for the project*
- *addressed security issues and conducted vulnerability assessment*

Page 18 changes

Sub-Teams. Team members may also form sub-teams that will focus on specifically defined tasks. Sub-teams may consist of people (one or more) from within the organization, or from outside sources such as consultants or contractors, that bring a specific expertise considered necessary to support the team's goals and objectives. These sub-teams may review issues such as:

- *Risk assessment (environmental, legal, political, technological, **security**, etc.)*
- *Technology assessment*
- *Site assessment*
- *Estimated market assessment*

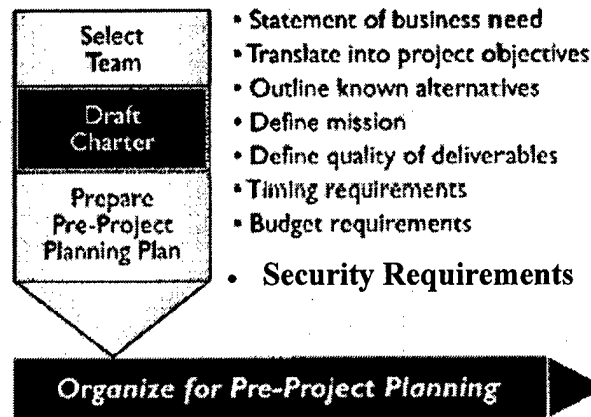
Page 20 changes

Anticipated Project Requirements/Skills and Staffing.

In developing the team, the team leader must evaluate project requirements and determine skill and staffing requirements for the following areas:

- *Quality*
- *Safety*
- *Security Manager/Specialist*

Page 26 changes



Page 31 changes

The Pre-Project Planning Plan. The pre-project planning plan is a formulation and documentation of the methods and resources an owner company can use to perform the pre-project planning process. It is composed of the following:

- *Defined Tasks of Minimizing Risks for:*
 - A. Research
 - B. Technology
 - C. Site
 - D. Market
 - E. Competition
 - F. Health and Safety
 - G. Security

Page 36 changes

As the team is formed, the core team leader or a representative must ensure that sufficient expertise is available to complete these activities. Special consideration should be given to the following:

- *Operations*
- *Project Estimating*
- *Risk Analysis*
- *Security Considerations*
- *Supply and Distribution*

Page 38 changes

The next step is to approach owners of the technologies of interest and request a limited secrecy agreement (if required). This will allow the team to exchange sufficient information for financial analysis, product evaluation, and process evaluation, as well as assessments of legal, patent, health, safety, **security**, toxicological, regulatory and environmental concerns.

Page 39 changes

An excellent time to review the criteria with management (i.e., the decision maker) and get feedback before proceeding with selection is after the selection criteria have been developed. Many times the selection criteria will be a weighted blend of the following:

- *Long-term competitive position*
- *Product qualities*
- *Process flexibility*
- *Financial analysis results*
- *Operating considerations*
- ***Security considerations***
- *Environmental considerations*
- *Compatibility with potential sites*

Page 43 changes

The function, *evaluate site(s)*, is the assessment of relative strengths and weaknesses of alternate locations to meet owner requirements. The theory of site selection is fairly simple - to find a location that maximizes benefits for the owner company. Practical application of the theory is less straightforward. Evaluation of site(s) may address issues relative to different types of sites, i.e., global region, country, local, **vulnerability assessment**, "inside the fence," or "inside the building."

Page 45 changes

If site selection is unconstrained by politics, legal, regulatory, financing requirements or social issues (which is highly unusual), then the selection will normally become an optimization based on best available choices. These generalized considerations are as follows:

- *Best overall economic choice (present plus future considerations)*
- *Best choice from a benefits standpoint (market)*
- *Best choice from a cost standpoint (raw materials, Labor, utilities, supply and distribution cost)*
- ***Best choice from a security standpoint***
- *Best choice from an initial investment standpoint*

Page 46 changes

Table 3.2: Site Objectives and Site Characteristics

SITE OBJECTIVES	SITE CHARACTERISTICS
Ability to Expand for Future Capacity	Hydrological Considerations
Level of Tax and Legal Considerations	Soil Capabilities
Long Range Goals	Roads
Access to Markets (New and Existing)	Equipment Foundations
Access to Low Cost Feed Stocks	Building Foundations
Access to Low Cost Construction Labor	Other Geotechnical Considerations
Access to Low Cost Operation Labor	Surface Run-off Considerations
Access to Low Term Growth Opportunities	Historical Implications
Land Availability and Costs	Environmental Evaluations
Transportation	Area Environmental Attainment
Competitor Considerations	Status
Energy Cost	Availability of Ambient Air Quality
Labor Analysis	Data
Availability	Feasibility of Providing NO offset
Background Checks	Surrounding Area Land Use
Work Ethics	Water Quality Permitting
Labor Posture	Hazardous Waste Clean Up
Labor Cost	Considerations
Skill Level	Location
Attitudes	Configuration
Regional Analysis	Topography
Ability to Attract and Retain	Zoning
Professional	Neighboring Land Use
Employees	Access (Road, Rail, Marine, Air)
Services	Construction Access
Infrastructure	Construction Feasibility
Quality of Life	Utilities
	Ownership

Utility Service and Cost Local Area Industry Size Local Area Industry Cost Local Area Financial Incentives Growth Incentives Taxes Environmental Restrictions Cost Analysis for Each Site Recurring Cost Non-recurring Cost Ability to Attract and Retain Professional Employees Overall Security Climate	Cost of Property Total Site Development Cost Weather Climate Security Implications
---	---

Page 51 changes

Table 3.3: Preliminary Information for Conceptual Scopes

Process Facilities	Buildings	Utility Projects
Design basis Heat and material balances Equipment list Flow diagram Plot plan Special provisions Cash flow Approval document Security Concerns Service and utility requirements and usage	Zoning Use Location Land requirements New/renovate Building population Environmental concerns Parking/landscaping Security concerns Design potential cost impact Roads and access Utilities Cafeteria/auditorium/laboratory requirements Telecommunications/sophistication of electronics Building type/finish/size/number of floors	Control philosophy Distributed control systems Environmental Noise limits/requirements Metering Safety concerns Basic layout Laws/standards/codes Cable trench interconnections Security Concerns Station ground interconnections Transformers/switch gear/disconnect switches Limits to high/low voltage connections

Page 55 changes

Other criteria have to be considered depending on political, social, and other economic factors. These factors may include the following:

- *Future access to market*
- *Future access to raw materials*
- *Long-term access to Labor skills needed*
- *Fit with company Long-range strategy*
- *Political considerations*
- *Transportation/communications/convenience*
- *Company image/quality of life/safety*
- *Environmental considerations*
- ***Security considerations***

Page 65 changes

The owner establishes the project conditions and it is in the owner's best interest to consider all potential areas of risk in the early stages of the concept and design phases. The business risk elements that deserve owner consideration include:

- *First costs (capital costs) - What is the worse case?*
- *Operating and maintenance costs*
- ***Security costs***
- *Start-up and commissioning costs*

Page 66 changes

In addition, there are a wide variety of construction related risks including:

- *Unforeseen economic factors (inflation, shortages, etc.)*
- *Differing site conditions*
- *Level of constructability*
- *Other global and logistical problems*
- ***Security risks***

Page 76 changes

Project Definition. The project definition describes the key technical and physical attributes of the project, including general quality requirements and budget, ~~or~~ commercial **or security** issues that would affect design planning and decision making.

Page 91 changes

The following are essential elements of the project definition package:

- *Project Objectives and Priorities. This section outlines the business needs and project aspects important to the owner. It includes the purpose for the project, cost/schedule trade-off criteria, operability, technology, **security**, project safety, environmental and other regulatory requirements, financial objectives, schedule objectives, quality requirements, community and governmental relations objectives, and operations requirements.*

Page 96 changes

Risk Assessment. Risk assessment is the result of identifying and assessing risks related to the project and of proactively seeking to minimize their impact on its success. Decision makers should assess all aspects of risk associated with an undertaking and tie this risk to the business needs of the enterprise. Risk assessment likely will include an analysis of the following:

- *Environmental Risks*
- *Social Risks*
- *Political Risks*
- *Processing Technology Risks*
- *Equipment Capability Risks*
- *Operational Risks*
- *Design Engineering Risks*
- *Project Estimate Risks*
- *Business Risks*
- ***Security Risks***

Page 116 changes

Security - includes all measures taken to guard against sabotage, crime, and attack that result in adverse impacts such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and offsite effects (consequences).

Page 120 changes

- 35. Detailed division of responsibilities matrix
- 36. Project procedure manual
- 37. Identification of standards and specifications to be used
- 38. Written vulnerability assessment**
- 39. Security plan change. Other team agreed to deliverables**

Page 121 changes

Design Basis

General

Plant Capacity Feedstocks;

Rate/Composition Design Yields and Variability

Product Streams; Rate(s) Service Factor Assumed

Plant Site Conditions Available

Economic Criteria

Security Criteria

Page 123 changes

Other details for a project report may include:

Contract change log summary

Expenditure and photographs, as appropriate commitment curves

Safety/accident experience

Security incidents

Page 124 changes

Capital Project Support Documents

Capacity effects - Discussion of present and planned capacity and timing of that capacity becoming available

Product quality effects - Discussion of change in product quality or product form as a result of this project

Health, safety, **security** and environmental considerations - Discussion of anticipated situation concerning health, safety, **security** and environment

Raw materials, supplies, inventory requirements - Listing of needs or change in needs

Page 126 changes

Table D.1. *Federal and Local Agencies and Statutes by Issue*

ISSUE AREA	FEDERAL		LOCAL	
	Agencies	Statutes	Agencies	Statutes
Air Contaminants	EPA OSHA	SARA Title III CAA	AQMD/APCDs Planning Depts. Fire Depts.	AQMD/APCD Rules Use Permit Codes Fire Dept. Regs
Environmental Impact	EPA Coast Guard DOT OSHA Army Corps of Engineers	NEPA CAA CWA	AQMD/APCDs Fire Depts. Planning Depts. Health Depts. Lead Agency (CEQN	Health Dept. Ordinances Land Use & User Permit Codes
Hazardous Waste & USTs	E P A DOT OSHA	TSCA RCRA CWA OSHA SARA Title II Hazardous Material Transport Regs	Health Depts. Fire Depts.	Health Depts. Ordinances Local UST Ordinances
Homeland Security	Dept. of Homeland Security FBI DoD FAA CDC		National Guard DPS/Police Fire Depts. Local Emergency Mgt. Health Depts.	

Appendix D: PDRI Updates

The following updates were made to CII Implementation Resource 113-2 "Project Definition Rating Index (PDRI), Industrial" (1996). Changes are indicated in bold and begin on page 37 of the implementation resource.

Page 37 changes

A. MANUFACTURING OBJECTIVES CRITERIA

A1. Reliability Philosophy

A list of the general design principles to be considered to achieve dependable operating performance from the unit. Evaluation criteria should include:

- ☐ Justification of spare equipment
- ☐ Control, alarm **security and** safety systems redundancy, and access control
- ☐ Extent of providing surge and intermediate storage capacity to permit independent shutdown of portions of the plant
 - ☐ **Assessment of extra capacity requirement if an area is sabotaged**
- ☐ Mechanical / structural integrity of components (metallurgy, seals, types of couplings, bearing selection, etc.)

A2. Maintenance Philosophy

A list of the general design principles to be considered to meet unit up-time requirements. Evaluation criteria should include:

- ☐ Scheduled unit / equipment shutdown frequencies and durations
- ☐ Equipment access **and control**/ monorails / cranes
- ☐ Maximum weight or size requirements for available repair equipment
- ☐ Equipment monitoring requirements (vibrations monitoring, etc.)

A3. Operating Philosophy

A list of the general design principles that need to be considered to support the routine scheduled production from the unit in order to achieve the projected overall on-stream time or service factor. Evaluation criteria should include:

- ☐ Level of operator coverage and automatic control to be provided
- ☐ Operating time sequence (ranging from continuous operation to five day, day shift only)
- ☐ Necessary level of segregation and clean out between batches or runs
- ☐ Desired unit turndown capability
- ☐ Design requirements for routine startup and shutdown
- ☐ **Design to provide security protection for material management and product control**

Page 39 changes

B. BUSINESS OBJECTIVES

B4. Affordability / Feasibility

Have items that may improve the affordability of the project been considered? These should include incremental cost criteria such as:

- ☐ Consideration of feedstock availability and transport to the job site, **especially during periods of elevated threat**
- ☐ Performing an analysis of capital and operating cost versus sales and profitability

Results of these studies should be communicated to the project team.

B6. Future Expansion Considerations

A list of items to be considered in the unit design that will facilitate future expansion. Evaluation criteria should include:

- ☐ Providing space for a possible new reactor train
- ☐ Providing tie-ins to permit a duplicate or mirror image unit that can be added without necessitating a shutdown

- ☐ Guidelines for over design of structural systems to allow for additions
- ☐ **Guidelines for design of security systems to allow for additions**
- ☐ **Guidelines for design that consider future expansion needs without compromising security**

Page 40 changes

B7. Expected Project Life Cycle

This is the time period that the unit is expected to be able to satisfy the products and capacities required. Have requirements for ultimate disposal and dismantling been considered? These requirements should include:

- ☐ Cost of ultimate dismantling and disposal
- ☐ Dismantling equipment requirements
- ☐ Presence of contaminants
- ☐ Disposal of hazardous materials
- ☐ Possible future uses
- ☐ **Consideration of security issues**

B8. Social Issues

Evaluation of various social issues such as:

- ☐ Domestic culture vs. international culture
- ☐ Community relations
- ☐ Labor relations
- ☐ Government relations
- ☐ Education / training
- ☐ Safety and health considerations
- ☐ **Security considerations**

C. BASIC DATA RESEARCH & DEVELOPMENT

C1. Technology

The chemistry used to convert the raw materials supplied to the unit into the finished product. Proven technology involves least risk,

while experimental technology has a potential for change.
Technology can be evaluated as:

- ☐ Existing / proven
- ☐ Duplicate
- ☐ New
- ☐ Experimental

Consider security aspects of technology selection, including proprietary technology. The technology choice can affect the security vulnerability.

Page 41 changes

C2. Processes

A particular, specific sequence of steps to change the raw materials into the finished product. Proven processes involve the least risk, while experimental processes have a potential for change. Processes can be evaluated as:

- ☐ Existing / proven
- ☐ Duplicate
- ☐ New
- ☐ Experimental

Consider security aspects of process selection, including proprietary processes. The process choice can affect the security vulnerability.

D. PROJECT SCOPE

D1. Project Objectives Statement (Y/N)

This is a mission statement that defines the project objectives, **including security considerations**, and priorities for meeting the business objectives. It is important to obtain total agreement from the entire project team regarding these objectives and priorities to ensure alignment.

D2. Project Design Criteria

The requirements and guidelines which govern the design of the project. Evaluation criteria should include:

- ☐ Level of design detail required
- ☐ Climatic data
- ☐ Codes & standards
 - ☐ National ☐ Local
- ☐ Utilization of engineering standards
 - ☐ Owner's ☐ Contractor's
 - ☐ Mixed
- ☐ **Evaluation of level of threat, conduct vulnerability and risk assessments.**

Page 42 changes

D3. Site Characteristics Available vs. Required (Y/N)

An assessment of the available vs. the required site characteristics.
Evaluation criteria should include:

- ☐ Capacity
 - ☐ Utilities ☐ Power
 - ☐ Fire water ☐ Pipe racks
 - ☐ Flare systems ☐ Waste treatment / disposal
 - ☐ Cooling water
 - ☐ Storm water containment system
- ☐ Type of buildings / structures
- ☐ Amenities
 - ☐ Food service ☐ Recreation facilities
 - ☐ Change rooms ☐ Ambulatory access
 - ☐ Medical facilities
- ☐ Product shipping facilities
- ☐ Material receiving facilities
- ☐ Material storage facilities
- ☐ Product storage facilities
- ☐ Security
 - ☐ Setbacks ☐ Access and egress
 - ☐ Sight lines ☐ Fencing, gates, and barriers
 - ☐ Clear zones ☐ Security lighting

D4. Dismantling and Demolition Requirements

Has a scope of work been defined for the dismantling of existing equipment and/or piping which may be necessary for completing new construction? Evaluation criteria should include:

- ☐ Timing
- ☐ Permits
- ☐ Approval
- ☐ Safety requirements
- ☐ **Security requirements**
- ☐ Hazardous operations
- ☐ Plant / operations requirements
- ☐ Narrative (scope of work) for each system
- ☐ Are the systems that will be dismantled...
 - ☐ Named & marked on process flow diagrams
 - ☐ Named & marked on P&ID's
 - ☐ Denoted on line lists and equipment lists
 - ☐ Denoted on piping plans or photo-drawings

Page 43 changes

D5. Lead / Discipline Scope of Work

This is a complete narrative description of the project, generally discipline oriented. This should be developed through the use of the Work Breakdown Structure (WBS) (Halpin et al. 1987). **Ensure that security assessment is part of WBS.**

E. VALUE ENGINEERING

E1. Process Simplification (Y/N)

Identify activities (through studies, reviews, etc.) for reducing the number of steps or the amount of equipment needed in the process in order to optimize performance **without compromising security.**

E2. Design & Material Alternatives Considered / Rejected (Y/N)

Is there a structured approach in place to consider design and material alternatives? **Has it been integrated with the security plan?** Has it been implemented?

E3. Design For Constructability Analysis

Is there a structured approach for constructability analysis in place?
Have provisions been made to provide this on an ongoing basis?
This would include examining design options that minimize construction costs while maintaining standards of safety, **security**, quality, and schedule.

Page 44 changes

F. SITE INFORMATION

F1. Site Location (Y/N)

Has the geographical location of the proposed project been defined? This involves an assessment of the relative strengths and weaknesses of alternate site locations. A site that meets owner requirements and maximizes benefits for the owner company should be selected. Evaluation of sites may address issues relative to different types of sites (i.e. global country, local, "inside the fence," or "inside the building"). This decision should consider the long-term needs of the owner company (CII 1995). The selection criteria should include items such as:

- ☐ General geographic location
 - ☐ Access to the targeted market area
 - ☐ Near sources of raw materials
 - ☐ Local availability and cost of skilled labor (e.g. construction, operation, etc.)
 - ☐ Available utilities
 - ☐ Existing facilities
- ☐ Land availability and costs
- ☐ Access (e.g. road, rail, marine, air, etc.)
- ☐ Construction access and feasibility
- ☐ **Security constraints**
- ☐ Political constraints
- ☐ Legal constraints

F4. Permit Requirements

Is there a permitting plan in place? The local, state, and federal government permits necessary to construct and operate the unit should be identified. These should include items such as:

- | | |
|---|------------------------------------|
| <input type="checkbox"/> Construction | <input type="checkbox"/> Fire |
| <input type="checkbox"/> Local | <input type="checkbox"/> Building |
| <input type="checkbox"/> Environmental | <input type="checkbox"/> Occupancy |
| <input type="checkbox"/> Transportation | <input type="checkbox"/> Special |

Be sure to investigate permitting restrictions related to security.

F5. Utility Sources With Supply Conditions

Has a list been made identifying availability / nonavailability, or **redundancy** of site utilities needed to operate the unit with supply conditions of temperature, pressure, and quality? This should include items such as:

- | | |
|---|---|
| <input type="checkbox"/> Potable water | <input type="checkbox"/> Instrument air |
| <input type="checkbox"/> Drinking water | <input type="checkbox"/> Plant air |
| <input type="checkbox"/> Cooling water | <input type="checkbox"/> Gases |
| <input type="checkbox"/> Fire water | <input type="checkbox"/> Steam |
| <input type="checkbox"/> Sewers | <input type="checkbox"/> Condensate |
| <input type="checkbox"/> Electricity (voltage levels) | |

F6. Fire Protection & Safety Considerations

A list of fire and safety related items to be taken into account in the design of the facility. These items should include fire protection practices at the site, available firewater supply (amounts and conditions), special safety **and security** requirements unique to the site, etc. Evaluation criteria should include:

- | | |
|---|---|
| <input type="checkbox"/> Eye wash stations | <input type="checkbox"/> Deluge requirements |
| <input type="checkbox"/> Safety showers | <input type="checkbox"/> Wind direction indicator |
| <input type="checkbox"/> Fire monitors & hydrants | devices (i.e. wind socks) |
| <input type="checkbox"/> Foam | <input type="checkbox"/> Alarm systems |

- ☐ Evacuation plan
- ☐ Security fencing

- ☐ Medical facilities

Page 52 changes

G. PROCESS / MECHANICAL

G8. Plot Plan

The plot plan will show the location of new work in relation to adjoining units. **It must consider security implications.** It should include items such as:

- ☐ Plant grid system with coordinates
- ☐ Unit limits
- ☐ Gates, fences and barriers
- ☐ Lighting
- ☐ Off-site facilities
- ☐ Tank farms
- ☐ Roads & access ways
- ☐ Roads
- ☐ Rail facilities
- ☐ Green space
- ☐ Buildings
- ☐ Major pipe racks
- ☐ Laydown areas
- ☐ Construction / fabrication areas

Page 55 changes

H. EQUIPMENT SCOPE

H1. Equipment Status

Has the equipment been defined, inquired, bid tabbed, or purchased?
This includes all engineered equipment such as:

- ☐ Process
- ☐ Electrical
- ☐ Mechanical
- ☐ HVAC
- ☐ Instruments

- ☐ **Security-related equipment**
- ☐ Specialty items
- ☐ Distributed control systems

Page 56 changes

I. CIVIL, STRUCTURAL, & ARCHITECTURAL

II. Civil / Structural Requirements

Civil / structural requirements should include the following:

- ☐ Structural drawings
- ☐ Pipe racks / supports
- ☐ Elevation views
- ☐ Top of steel for platforms
- ☐ High point elevations for grade, paving, and foundations
- ☐ Location of equipment and offices
- ☐ Construction materials (e.g. concrete, steel, client standards, etc.)
- ☐ Physical requirements
- ☐ Seismic requirements
- ☐ Minimum clearances
- ☐ Fireproofing requirements
- ☐ Corrosion control requirements / required protective coatings
- ☐ Enclosure requirements (e.g. open, closed, covered, etc.)
- ☐ Secondary containment
- ☐ Dikes
- ☐ Storm sewers
- ☐ Client specifications (e.g. basis for design loads, **vulnerability and risk assessments**, etc.)
- ☐ Future expansion considerations

I2. Architectural Requirements

The following checklist should be used in defining building requirements.

- ☐ Building use (e.g. activities, functions, etc.)
- ☐ Space use program indicating space types, areas required, and the functional relationships between spaces and number of occupants
- ☐ Service, storage, and parking requirements
- ☐ Special equipment requirements
- ☐ Requirements for building location / orientation
- ☐ Nature / character of building design (e.g. aesthetics, **crime prevention through environmental design (CPTED)** etc.)
- ☐ Construction materials
- ☐ Interior finishes
- ☐ Fire resistant requirements
- ☐ Explosion resistant requirements
- ☐ "Safe haven" requirements
- ☐ Acoustical considerations
- ☐ Safety, security / **vulnerability**, and maintenance requirements
- ☐ Fire detection and / or suppression requirements
- ☐ Utility requirements (i.e. sources and tie-in locations)
- ☐ HVAC requirements
- ☐ Electrical requirements
 - ☐ Power sources with available voltage & amperage
 - ☐ Special lighting considerations
 - ☐ Voice and data communications requirements
 - ☐ UPS and / or emergency power requirements
- ☐ Outdoor design conditions (e.g. minimum and maximum yearly temperatures)

J. INFRASTRUCTURE

J1. Water Treatment Requirements

Items for consideration should include:

- ☐ Wastewater treatment
 - ☐ Process waste
 - ☐ Sanitary waste
- ☐ Waste disposal
- ☐ Storm water containment & treatment
- ☐ **Security breach through storm water system or waste connections**

J2. Loading / Unloading / Storage Facilities Requirements

A list of requirements identifying raw materials to be unloaded and stored, products to be loaded along with their specifications, and Material Safety Data Sheets. This list should include items such as:

- ☐ Instantaneous and overall loading / unloading rates
- ☐ Details on supply and / or receipt of containers and vessels
- ☐ Storage facilities to be provided and / or utilized
- ☐ Specification of any required special isolation provisions
 - ☐ Double wall diking and drainage
 - ☐ Emergency detection (e.g. hydrocarbon detectors / alarms)
 - ☐ Leak detection devices or alarms
- ☐ **Essential security considerations should include:**
 - ☐ **Inspections**
 - ☐ **Secure storage**
 - ☐ **Authorized deliveries**
 - ☐ **Access/egress control**

J3. Transportation Requirements (Y/N)

Specifications identifying implementation of "in-plant" transportation (e.g. roadways, concrete, asphalt, rock, etc.) as well as methods for receiving / shipping/storage of materials (e.g. rail, truck, marine, etc.).

Page 60 changes

K. INSTRUMENT & ELECTRICAL

K4. Substation Requirements / Power Sources Identified

Substation requirements should include the following:

- ☐ Number of substations required
- ☐ Electrical equipment rating required for each substation
- ☐ Specifications for all major electrical substation equipment
- ☐ Infrastructure required for each substation considering building type and environment, fencing, access, **and if applicable lighting and barriers**, and substation yard materials

Page 61 changes

K6. Instrument & Electrical Specifications

These specifications should include items such as:

- ☐ Distributed Control System (DCS)
- ☐ Instrument data sheets
- ☐ Motor control and transformers
- ☐ Power and control components
- ☐ Power and control wiring (splicing requirements)
- ☐ Cathodic protection
- ☐ Lightning protection
- ☐ **Security systems**
- ☐ Grounding
- ☐ Electrical trace
- ☐ Installation standards
- ☐ Lighting standards **to include security**
- ☐ Civil requirements for electrical installation
 - ☐ Protection / warning for underground cabling
 - ☐ Special slabs or foundations for electrical equipment

L. PROCUREMENT STRATEGY

L2. Procurement Procedures and Plans

Specific guidelines, special requirements, or methodologies for accomplishing the purchasing, expediting delivery, **and security** of equipment and materials required for the project. Evaluation criteria should include:

- ☐ Listing of approved vendors
- ☐ Client or contractor paper?
- ☐ Reimbursement terms and conditions
- ☐ Guidelines for supplier alliances, single source, or competitive bids
- ☐ Guidelines for engineered / field contracts
- ☐ Who assumes responsibility for owner-purchased items?
 - ☐ Financial
 - ☐ Shop inspection
 - ☐ Expediting
- ☐ Tax strategy
 - ☐ Engineered
 - ☐ Field materials
 - ☐ Labor
- ☐ Definition of source inspection requirements and responsibilities
- ☐ Definition of traffic / insurance responsibilities
- ☐ Definition of procurement status reporting requirements
- ☐ Additional / special owner accounting requirements
- ☐ Definition of spare parts requirements
- ☐ Local regulations (e.g. tax restrictions, tax advantages, etc.)
- ☐ **Additional/special owner security requirements**

Page 63 changes

M. DELIVERABLES

M1. CADD / Model Requirements

Computer Aided Drafting and Design (CADD) requirements should be defined. Evaluation criteria should include:

- ☐ Software system required by client (e.g. AutoCAD, Intergraph, etc.)
- ☐ Will the project be required to be designed using 2D or 3D CADD?
- ☐ If 3D CADD is to be used, will a walk through simulation be required?
- ☐ Application software (e.g. ADEV Pro-series, Cadpipe, PDS, etc.)
- ☐ Owner / contractor standard symbols and details
- ☐ How will data be received and returned to / from the owner?

Security provisions?

- ☐ Disk
- ☐ Electronic transfer
- ☐ Tape
- ☐ Reproducibles

Page 64 changes

M3. Distribution Matrix (Y/N)

A distribution matrix (**document control system**) identifies most correspondence and all deliverables. It denotes who is required to receive copies of all documents at the various stages of the project, **and ensures the proper distribution of documentation.** Some documents may be restricted due to security concerns.

P. PROJECT EXECUTION PLAN

P2. Engineering / Construction Plan & Approach

This is a documented plan identifying the methodology to be used in engineering and constructing the project. It should include items such as:

- ☐ Responsibility matrix
- ☐ Contracting strategies (e.g. lump sum, cost-plus, etc.)
- ☐ Subcontracting strategy
- ☐ Work week plan / schedule
- ☐ Organizational structure
- ☐ Work Breakdown Structure (WBS)
- ☐ Construction sequencing of events
- ☐ Safety requirements / program
- ☐ **Security requirements / program**
- ☐ Identification of critical lifts and their potential impact on operating units
- ☐ QA / QC plan

P4. Pre-Commissioning Turnover Sequence Requirements

This defines the owner's required sequence for turnover of the project for pre-commissioning and startup activation. It should include items such as:

- ☐ Sequence of turnover
- ☐ Contractor's required level of involvement in pre-commissioning
- ☐ Contractor's required level of involvement in training
- ☐ Contractor's required level of involvement in testing
- ☐ Clear definition of mechanical / electrical acceptance requirements
- ☐ **Clear definition of security system acceptance requirements**

Page 67 changes

P5. Startup Requirements

Have the startup requirements been defined and responsibility established? **Identify the sequence that activates heightened security requirements for the facility.**

P6. Training Requirements

Have the training requirements been defined and responsibility established? **Identify the security training requirements for the operational facility.**

Appendix E: Alignment Updates

The following updates were made to CII Implementation Resource 113-3 “Alignment During Pre-Project Planning” (1997). Changes are indicated in bold.

Page 1 changes

1.1. Definition of Alignment

As with any concept, a clear and specific definition is required so that the discussion can begin from a common starting point. *Webster’s Dictionary* defines alignment as: “The condition of being in satisfactory adjustment or having the parts in proper relative position.” The following definition of alignment provides a framework for the information presented in this implementation resource. In the context of capital projects, alignment may be defined more specifically as:

The condition where appropriate project participants are working within acceptable tolerances to develop and meet a uniformly defined and understood set of project objectives.

These project objectives must meet business or mission requirements, **including security**, and the overall organization’s strategy. They are formed in the early stages of project development and have a critical impact on the success of the project delivery process.

Page 4 changes

CII defines pre-project planning as *the process of developing sufficient strategic information with which owners can address risk and decide to commit resources to maximize the chance for a successful project*. Pre-project planning has many aliases such as front-end loading, front-end planning, feasibility analysis, programming, conceptual planning, and others. **It includes elements such as a vulnerability assessment.** Pre-project planning, in effect, bridges the gap between business planning and detailed design. Previous CII research has shown that good pre-project planning improves project performance.

Page 6 changes

The business environment under which projects are planned and executed is increasingly more integrated. Projects are developed using a wide range of relationships including joint ventures, partnerships with government, formal contracts, and associations of companies within the same industry. Mixed in with the formal relationships are the concerns of informal stakeholders such as government regulatory agencies and the public. **Increasing attention to the requirements of effective security add to project complexity.** As a result, a relatively simple project may have a large number of stakeholders. Obviously those different stakeholders will frequently have conflicting objectives for the same project.

Page 17 changes

How Open and Effective Communication Affects Alignment

Communication includes all the activities and behaviors by which information or ideas are transferred to others. Communication during the pre-project planning phase is difficult for reasons such as the iterative nature of the pre-project planning process, the large amount of stakeholder involvement, the relative “non-dimensional” nature of the work, and so on. The early planning phase of a project is characterized by many decisions that will significantly affect the entire project. Examples include site selection, technology alternatives, execution approaches, **security considerations**, and trade-offs between cost and schedule constraints. Communication is critical because on most projects this is a period of dramatically changing scope, limited amounts of time, and resources available.

Page 22 changes

Key Execution Process Issue #1: Stakeholders are appropriately represented on the project team.

The pre-project planning team should include representatives from all significant project stakeholders. Stakeholders are defined as those directly or indirectly associated with the project, those affected by the project and its activities, and those interested in the outcome of the project. The team needs to include representatives from operations, construction, business management, **security**, and other stakeholder groups as well as project management and

engineering, **as appropriate**. Those projects involving joint ventures, complex internal business organizations, or outside consultants should be especially cognizant of this issue.

Page 24 changes

Appropriate Stakeholder Representation: Recommended Practices

The project manager, with sponsor support, should appoint representatives from each of the project stakeholder groups. These individuals should be at the right level within the organization. It is especially important to get representation from business, operations, **security**, and technology in addition to project management. A difficulty is to keep the team small enough to be productive, but inclusive enough to insure buy-in from as many stakeholders as possible.

Table 2.1. Example Stakeholder Groups

<p>BUSINESS:</p> <ul style="list-style-type: none"> • Business and Market Evaluation • Financial Analyst • Human Resources • Labor Relations • Legal Advisor • Project Sponsor • Public Relations 	<p>PROJECT MANAGEMENT:</p> <ul style="list-style-type: none"> • Cost and Schedule • Environment • Estimating • General Engineering • Project Controls • Process Engineering • Project Manager • Quality/Inspection
<p>OPERATIONS:</p> <ul style="list-style-type: none"> • Facility Operations • Maintenance • Procurement • Research and Development • Security • Safety • Warehousing 	<p>OTHERS:</p> <ul style="list-style-type: none"> • Construction • General Public • Information Management • Specialist Engineering

Factors that affect team composition include the size of the project, resources available, degree of participation desired, the degree of pre-project planning detail desired, and project specific objectives. **The vulnerability assessment should also be a factor in stakeholder selection.**

Other Related Execution Process Issues

A project team may also wish to evaluate its performance in these areas:

- *Process for identifying project objectives.* Project objective setting is extremely important in ensuring that the project meets the business or mission needs of the facility. Having a standard process that develops objectives is important. **Security should be a part of project objectives.**
- *Involvement by outside contractors.* Outside contractors bring additional expertise and perspective into the project. Structured outside review and participation provides an avenue to perform tasks that may not be possible by in-house personnel.
- *Involvement by operations.* Operations personnel will have a say in the project at some time during its life. Having a structured (meaningful) review process by operations during pre-project planning should reduce changes later and improve commitment and alignment throughout project execution.
- *Involvement by security.* **Security affects each project stage from pre-project planning through operations to decommissioning. Consideration of security threats and responses at each stage of planning and execution is essential to project success.**

Page 32 changes

Key Information Issue: The priority between the costs, schedule, and required project features is clear.

Many other important elements of information are provided by the project sponsor, but the priority between cost, schedule, and required features most affects team alignment and project success. Information such as project safety goals, project quality goals, **security requirements**, the products to be produced by the facility, schedule constraints, budget constraints, required production capacity, and site selection criteria are examples of other important elements of information needed by the team.

Page 33 changes

The CII Agreement Matrix is an efficient tool for identifying, prioritizing, communicating, reinforcing, and controlling project objectives. This tool quantifies agreement between various project participants. (CII Publication 12-1, *Setting Project Objectives*, provides a complete description of the development and uses of the Agreement Matrix.) **Security is a priority that must be addressed. By conducting a comprehensive vulnerability assessment during the initial stages, project leaders can determine appropriate security measures required at each stage of project development.**

Page 62 changes

The future only points to more competition, more limits on available resources, more pressure on capital budgets, **and a greater focus on security.** Better pre-project planning will help teams succeed in this difficult environment and produce the correct project within budget and on schedule.

Appendix F: Design Effectiveness Updates

The following updates were made to CII Research Summary 8-1 "Design Effectiveness" (1986). Changes are indicated in bold and begin on page 5.

Page 5 changes

4: DESIGN EVALUATION CRITERIA

The seven criteria most suited for an initial evaluation of design effectiveness are summarized in Figure 1. Each criterion is essential to each design user, and can be evaluated during or immediately after completion of project construction. Not all of these criteria are easily quantified by measurable factors. Figure 1 also shows which of these seven criteria are in large part quantifiable or must be subjectively rated by personal judgment. Although subjective ratings are valuable, methods should be pursued to develop quantitative evaluations for all criteria.

These seven criteria are not all-inclusive for measuring design effectiveness. **If the Vulnerability Assessment indicates that security is an essential element of the project, add Security as a criterion in the Objective Matrix.** Other criteria relating to operability, maintainability, safety, plant operating efficiency, and plant performance are at least of equal importance. These latter criteria, however, require evaluations after a period of plant operation and by different personnel than those involved in a project's design, construction, and start-up. Thus, they are not included in this publication. The seven criteria included in Figure 1 can be evaluated before the project team disperses and important data become unavailable.

CRITERIA		
	Quantitative	Subjective
Accuracy of Design Documents	X	
Usability of Design Documents		X
Cost of Design Effort	X	
Constructability of Design		X
Economy of Design		X
Performance Against Schedule	X	
Ease of Start-Up	X	
Security	X	

Figure 1. Initial Design Evaluation Criteria

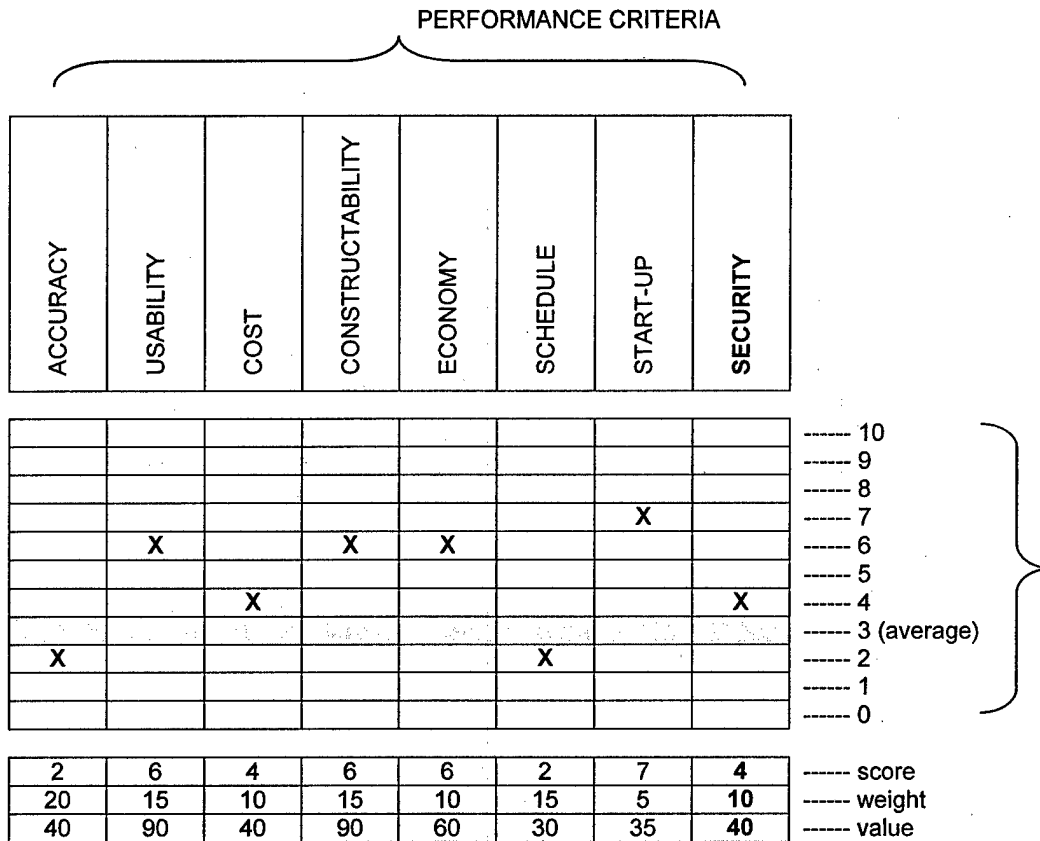
Page 8 changes

Ease of Start-Up

The ease of start-up is a partial indication of the accuracy and efficiency of the design. A measure of the efficiency is obtained by comparing budgeted to actual start-up time. The number of operators and maintenance personnel required during start-up can also be an indicator of the ease of start-up.

Security

Security throughout the project life cycle is directly linked to the effectiveness of the design effort. A quality design considers this element throughout the project. Security considerations are derived from the vulnerability assessment. An effective design will help decrease associated security vulnerabilities.



INDEX

425

Figure 2. Design Evaluation Matrix

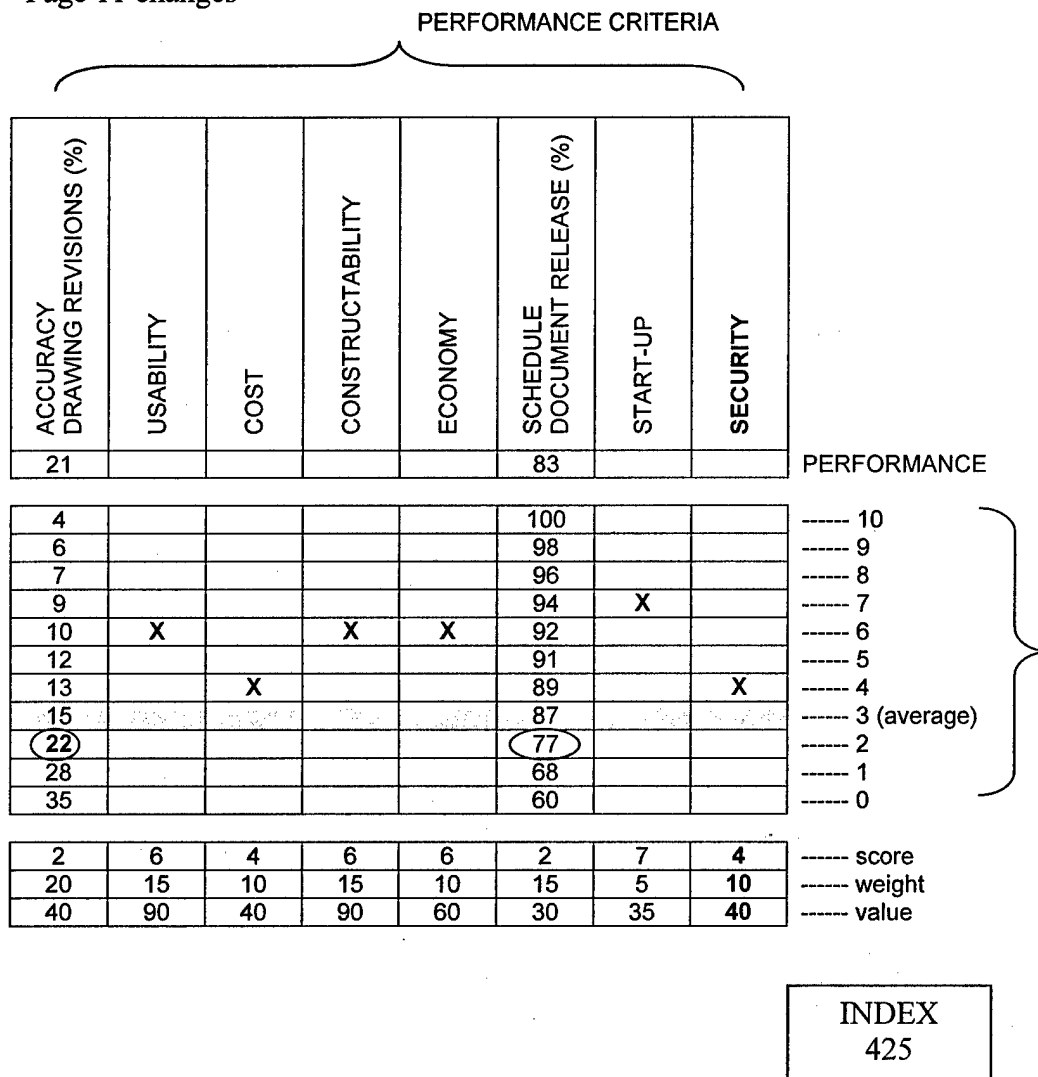


Figure 3. Design Matrix Using Quantitative Evaluation

Appendix G: Constructability Updates

The following updates were made to CII SP 34-2 "Constructability Implementation Guide" (1993). Changes are indicated in bold.

Page 2 changes

Constructability: A Mechanism for Success

CII defines constructability as "the optimum use of construction knowledge and experience in planning, design, procurement, and field operations to achieve overall project objectives."

Why pursue constructability? The task force suggests that constructability can support all project objectives: reduced cost, shortened schedules, improved quality, **security**, and safety, and enhanced management of risk.

Early constructability efforts result in a payback, but how large of a payback is possible? CII research has cited cost reductions of between 6 and 23 percent, benefit/cost ratios of up to 10 to 1, and significant schedule reductions. One of the case studies presented in this Guide cites total installed project cost savings of 1.1 percent with a benefit/cost ratio of 10 to 1, and a 10 percent reduction in project duration. These benefits establish a significant motive for pursuing constructability.

Page 22 changes

The intangible benefits from constructability are as important as the quantitative benefits, and must be recognized accordingly. These include more accurate budgets and schedules, improved site layouts, improved project team relationships, more repeat work, **improved security**, and many others.

As many constructability benefits were not tracked on these projects, savings went beyond those items that were documented. Therefore, the documented numbers may underestimate the true benefits of constructability. Additional qualitative benefits recognized on these projects included constructability-produced improvements to such items as safety, **security**, schedule, cost, and

quality. Further discussion of these case studies may be found elsewhere in this publication

Page 27 changes

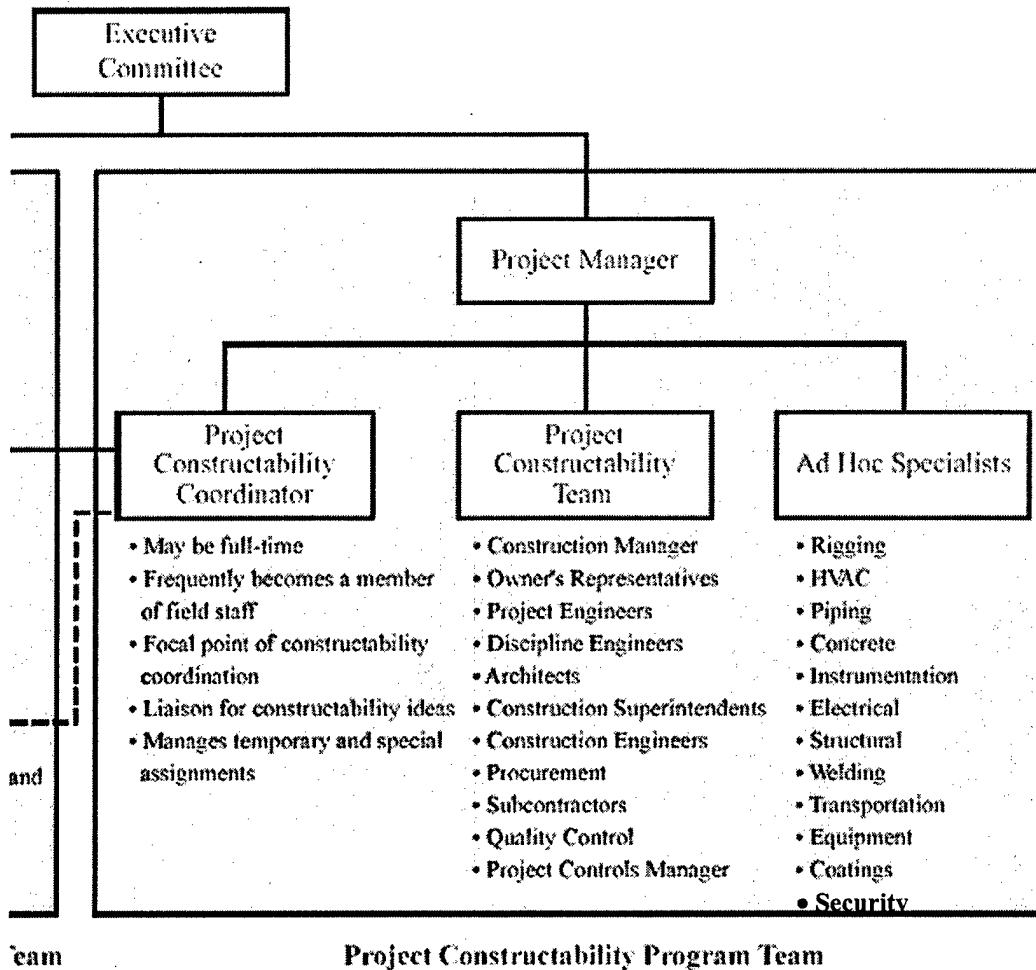


Figure 2.2. Constructability Organizational Structure (Tool 12)

Page 30 changes

Suggested information fields for each record in the database include the following:

- Short descriptive title of the idea
- Detailed idea description
- Discipline/work area category and subcategory (e.g., piping: fabrication, or electrical; conduit, etc)
- Pertinent project phase (e.g., detailed design, procurement, field construction, etc)
- Primary effects on project (e.g., cut cost, shorten duration, reduce work-hours, improve safety, **improve security**, eliminate materials, etc)
- Needs for updating/modifying corporate standard specifications
- Projects using this idea
- Personal contacts for more information
- Referenced manufacturer's literature

The database should be available in both hard copy and computer file formats. The hard copy format should contain a complete, detailed, and accurate table of contents.

Page 33 changes

Select owner project manager committed to constructability. The project manager (PM) from the owner's organization plays a vital role in the decision to implement a project-level constructability program. In addition, the emphasis the PM places on the program impacts its effectiveness. Without the PM's commitment, making constructability a positive influence will be extremely difficult. The project manager must be able to lead the team in the following areas:

- *Establish a supportive project environment.* The roles, responsibilities, actions, and lines of communication for the project's team need to provide for early and meaningful construction knowledge and experience
- *Make a commitment to increased cost effectiveness.* Constructability will be enhanced if the project manager emphasizes the influence that project decisions have on the project's cost. The project manager can insist that construction input be provided for in the project's major decisions
- *Use constructability to meet other project objectives.* Constructability should support the traditional project objectives of cost, schedule, quality, **security** and safety. Constructability also can be used to provide trade-offs between conflicting objectives.

Page 35 changes

Establish project objectives considering constructability. Constructability plays an important role in fulfilling established project objectives. Developing a clear understanding of the project's objectives and priorities is the first responsibility of the owner's team in constructability improvement. The project objectives typically include cost, schedule, quality, **security** and safety. Other objectives for various projects include: reliability, aesthetics, leaseability, public image, operability, and maintainability. As illustrated in the case studies presented in the appendix, constructability programs can reduce maintenance costs, increase operability, and increase safety.

Page 36 changes

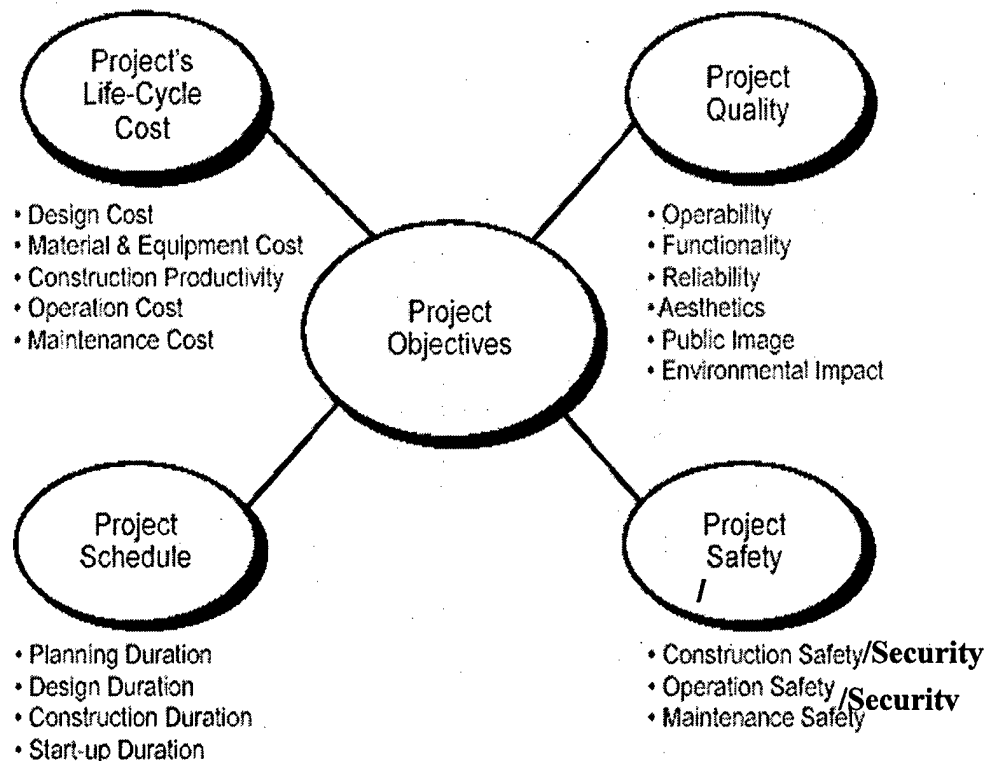


Figure 3.3. Traditional Project Objectives

Page 37 changes

Establish constructability objectives. Once the design and construction participants are involved, a specific set of constructability objectives can be developed. This set of objectives can be used to enable trade-off analysis between constructability and other project considerations, **such as security.**

Page 48 changes

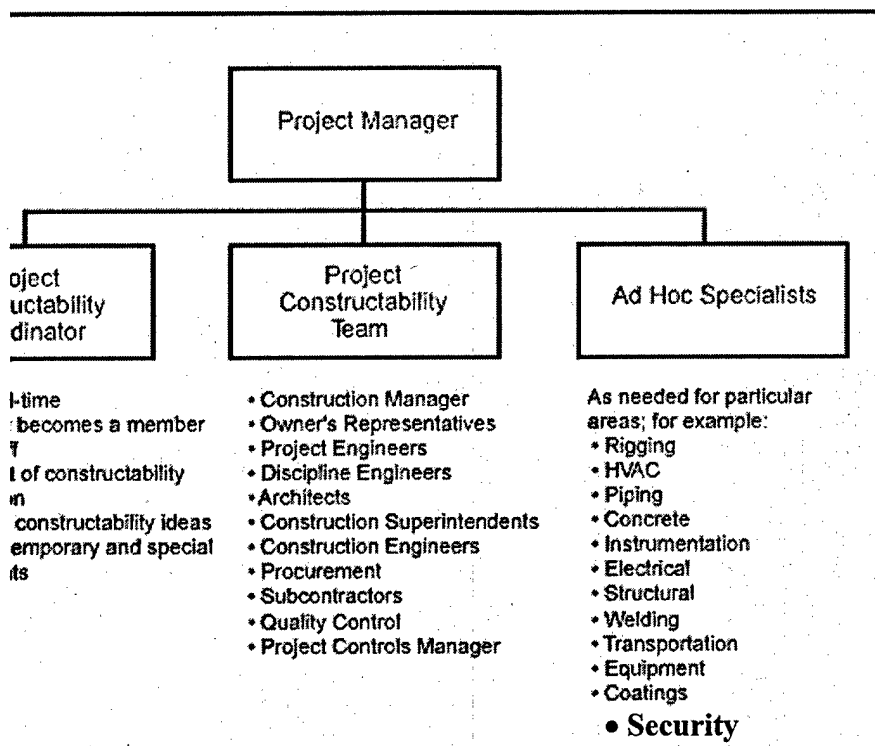


Figure 4.2. Sample Project Organization Structure

Page 103 changes

Constructability Program Scope

The engineer/contractor (or engineer/constructor or engineer/construction manager) shall develop a Project Specific Constructability Program. The minimum requirements for this program are:

1. Development of the construction execution plan for integration into the project execution plan.
2. Participation in the development of the project contracting and procurement strategy with the other members of the project team and develop the contracting/subcontracting plan which results from this strategy.
3. Identification of major or special construction methods for incorporation into the basic design approach.
4. Development of construction logic and activity durations for the project plan in order to achieve a construction driven project schedule.
5. Participation in the development of project estimates and budgets.
6. Development of a site logistics plan.7. Participation in site arrangement studies, when required, to insure access for plant equipment and construction equipment.
8. Participation in building arrangement studies, when required, to insure access for construction personnel, materials, and plant equipment.
9. Development of the methods for constructability input into the design process
10. **Consideration of site security plan, as it may affect construction and ongoing operations.**

Page 107 changes

The constructability surrogate shall develop a project specific constructability program. The minimum requirements for this program are:

- a. Development of the construction execution plan for integration into the project execution plan.
- b. Participation in the development of the project contracting and procurement strategy with the other members of the project team and develop the contracting/subcontracting plan which results from this strategy.
- c. Identification of major or special construction methods for incorporation into the basic design approach.

- d. Development of construction logic and activity durations for the project plan in order to achieve a construction drive project schedule.
- e. Participation in the development of project estimates and budgets.
- f. Development of a site logistics plan.
- g. Participation in site arrangement studies, when required, to insure access for plant equipment and construction equipment.
- h. Participation in building arrangement studies, when required, to insure access for construction personnel, materials, and plant equipment.
- i. Development of the methods for constructability input into the design process.
- j. **Consideration of site security plan, as it may affect construction and ongoing operations.**

Page 109 changes

Tool 17

I-1 Constructability Program is an integral part of PEP HIGH

I-2 Project planning involves construction knowledge and experience HIGH

- Planning aspect requires security input
- Security factors affect construction
 - Site selection
 - Establishment of relative priorities
 - Preferred suppliers

I-5 Basic design approaches consider major construction methods HIGH

- Implications of major construction methods on security
 - Modularization can increase security
 - Reduce on-site labor force
 - Decrease visibility of efforts

I-6 Site layouts promote efficient construction HIGH

- Site layout decisions can affect security
- Adherence to security standards
 - Efficient access control procedures
- Retrofit vs. Greenfield

I-7 Project team participants responsible for constructability are identified early-on HIGH

II-6 Designs promote construction accessibility of personnel, material, and equipment HIGH

- Construction expertise not usually available during pre-project planning

I-4 Project schedules are construction-sensitive MED

- More of an issue for retrofit
 - When will you gain access to certain areas

I-8 Advanced information technologies are applied throughout project MED

- Security implication of technologies

II-2 Designs are configured to enable efficient construction MED

II-4 Construct MED

- Specs promote security

II-5 Module/preassembly designs are prepared MED

II-7 Designs and plans facilitate construction MED

- Adverse weather effects

II-9 Security during construction is enhanced

Appendix H: Materials Management Updates

The following updates were made to Implementation Resource 7-3 "Procurement and Material Management: A Guide to Effective Project Execution" (1999). Changes are indicated in bold.

Chapter 1: The Evolution of Construction Project Materials Management

Section 1.0

The team determined that a security introduction should be added but did not draft the words

Section 4.0 Current Trends

The team determined that security trends should be added but did not outline specific trends

Section 4.1

Page 1-8 changes

...governmental organizations. **With the Internet outgrowth, information security is a major issue that needs to be addressed.**

Chapter 2: Project Materials Management Planning Guide

Page 2-3 changes

2.0 Project Definition and Strategy Development

2.1 General

The materials plan must fit within the framework of the overall project plan and take into account the limitations, constraints, and overall project strategies. Before the materials plan can be developed, certain basic project information is required. General project descriptions and parameters such as type, size, and location will begin to define the overall project plan. Those responsible for materials management should be identified at this stage and actively participate in the

development of the various project strategies. Some of the more significant strategic elements are:

- Use of existing materials.
- Approach to procurement of critical equipment **and identification of special security needs.**

Page 2-5 changes

2.2.2 Project Location

The project location provides the basis for site access planning and is necessary for initial investigation of possible local suppliers, fabrication shops, and subcontractors. Project location will also influence the extent of preassembly and modularization, mode of transport, permits, and in general, the entire transportation plan. Location will have an impact on method of storage and disposal of certain materials (e.g., hazardous) and may require special permits and licenses. Suppliers providing such services may be specified as sole source by local or state governments.

Actual jobsite conditions are an important consideration. Access to the site, total area available for storage, condition and layout of site roads, **security consideration**, and numerous other details have a significant impact on materials planning.

Page 2-6 changes

2.3.2 Owner's Role

The most substantial impact owners can have on successful materials management is simply how much emphasis they place on this area of project management. Owners must ensure that materials management is recognized as a critical project management function by both their own organization and by the engineering and construction contractors. By stressing the importance of materials management activities and by setting specific criteria for evaluating proposed systems, **and the security thereof**, the owner will establish a solid foundation for carrying out the materials management function.

Page 2-9 changes

2.4 Business Considerations

Significant outside factors, typically beyond the control of the project team, can have a major impact on the project. The principal points usually include

economic and market conditions that affect the cost and availability of needed labor, services, equipment, security, and materials. **The SVA may identify local security concerns that affect overall project cost.**

Page 2-10 changes

There are other factors that may contribute to the analysis and decision for extensive prefabrication including:

- Equipment.
- Safety.
- **Security.**
- Schedule.

Page 2-16 changes

- Early Involvement
- **Security – is the material hazardous, highly pilferable, or a critical asset of the completed project?**

Page 2-20 changes

3.4.4. Schedule Implications

Although there have been attempts to develop formulas for calculating the amount to be purchased in an “initial bulk buy,” there are none that effectively do the job consistently. Factors that must be considered in determining the initial quantities include:

- Stability of engineering design.
- Materials availability.
- Transportation constraints.
- **Security consideration.**

Page 2-23 changes

3.5 Planning for Prefabricated Materials

3.5.1 General

Prefabricated materials typically include packaged equipment, modules, and preassemblies (i.e., structural steel, pipe spools, electrical, and instrument control stations). Materials management planning is usually more complex with extensive prefabrication because it introduces another level of control/**security due to a** different site, the fabricator's shop.

Page 2-24 changes

Modules and preassemblies require special consideration because of the level of design and bulk materials involved. Highly prefabricated facilities can involve hundreds of modules. Some international projects procure essentially all process facilities in the form of modules. **Security assurance of these items is a concern for prefabrication through shipment installation.**

Page 2-25 changes

3.5.4 Source of Materials

There are two approaches in acquiring bulk materials for prefabricated materials. In one case, the prime contractor buys the bulk materials and delivers them to the fabricator. In the other, the fabricator supplies the bulk materials in the same way it supplies fabrication services. Often a mix of the two will need to be employed. Process equipment for modules is usually purchased by the engineer. Considerations in determining the approach are:

- Cost of materials.
- Materials availability and lead times.
- Volume of quantities required.
- Uniqueness of materials (e.g., fiberglass, plastic lined pipe).
- **Level of control and security desired (especially for high cost materials).**

Page 2-26 changes

4.2 Approved Suppliers List

After defining purchasing responsibilities, the Approved Manufacturers List (AML) and/or Approved Suppliers List (ASL) must be prepared. **Security factors should be considered in reviewing the AML/ASL.**

Page 2-28 changes

4.3 Terms and Conditions

Standard purchase order terms and conditions (T&Cs) should be developed for use on the project. A variety of questions must be addressed concerning any existing T&Cs such as:

- Are indemnity clauses, Alternative Dispute Resolution clauses, warranties, and performance requirements adequate?
- Is the project fully funded or do special cancellation clauses need to be added?
- Is patented technology being procured which require special clauses?
- **How will security be provided for sensitive materials?**

Page 2-39 changes

6.5 The Inspection Plan

Planning for inspection evolves through the design, pre-award, and post-award phases and includes the following general functions:

- Evaluating the need for in-plant inspection: this determination is made early in the engineering and procurement cycle, where the equipment and material is being specified. In-plant inspection will generally be limited to engineered items, permanent plant equipment, and critical fabricated materials that are:
 - Complex and/or costly.
 - Critical to the safe , **secure**, and reliable operation of the facility.

Page 2-40 changes

7.2 F.O.B. Terms and INCOTERMS

F.O.B. means "free on board." However, for the purpose of logistics planning and execution, the term denotes the point at which ownership of material, **as well as security responsibility**, transfers to the buyer

Page 2-41 changes

Some of the more important transportation and logistics planning elements are:

- Remoteness of jobsite
- Locations of in-transit fabrication facilities as applicable
- Sensitivity/**security** of cargo

Page 2-42 changes

Prior to approaching carriers to discuss a national or project agreement, the owner or contractor should have an estimated volume of shipments, definition of its service expectations, and a scope of requirements to be met over the life of a project/contract. The contract negotiated should be unambiguous and specific in matters such as scope definition, service level requirements, **security requirements**, and pricing.

Page 2-43 changes

7.8 Courier Service

Planning should consider those carriers capable of providing overnight or express delivery using company owned and controlled equipment at competitive pricing. To some jobsites, ground services may provide all the services required at a more competitive price than carriers specializing in overnight delivery. **Security requirements may be a consideration in carrier selection.** Delivery plans should also be established for drawings and documents that are not time-sensitive. U.S. mail service should be used when time permits. Increasingly, electronic mail, electronic data interchange (EDI), and electronic transmittal of project documents are the norm, **but security aspects should be considered.**

7.9 Site Personnel Logistics

Remote site personnel transportation can present unique concerns to the transportation/logistics personnel. Alternatives of chartered air, ferry, and dedicated bus service should be considered, **as well as their security implications.** Planning should include discussions with local authorities to ensure plans do not adversely affect the environment or the local community.

Page 2-44 changes

7.10 Special Loads

In order to determine maximum size envelope for special loads (i.e., vessels, skids, packaged equipment, and modules), it is necessary to determine requirements for route permits and/or clearances from manufacturers' facilities to the jobsite. Utilizing the services of reputable transportation company (truck and rail) personnel familiar with the routes/**security** can greatly reduce the time required to accomplish this task.

Page 2-47 changes

On large projects, proper reporting and control can usually be achieved using a fully integrated materials management system augmented with the generation of exception reports such as:

- Late shipments
- Oversized loads
- Critical material deliveries
- Three-month shipping reports (90-day forecasts)
- Alert reports
- **Security breaches**

Page 2-49 changes

8.2 Site Access Security

In order that security during construction can be effectively enforced, site security planning includes determining the best location for perimeter fencing, gates, security lighting, parking, **access control**, and other facilities.

Page 2-51 changes

8.5.2 Warehousing Facilities and Storage

Planning warehouse space and layout is influenced by a number of variables **including availability, location, and security**

Page 2-52 changes

8.6 Equipment Storage Protection/Maintenance

Plant equipment and materials require varying degrees of protection and maintenance **or security** from the time of arrival at the project-site until either installation or initial plant operation

Storage categories can be generally classified as:

- Materials that require extraordinary protection (e.g., filtered, temperature, **high security**, and humidity controlled environment).

Page 2-55 changes

8.9 Surplus

Surplus materials are the result of:

- Design changes.
- Errors in estimates and takeoff.

- Improper site warehousing.
- Duplicate buying efforts.
- Inventory errors.
- Poor field control of issued materials.

Site materials personnel must be prepared to deal with all surplus, **including security and accounting concerns.**

Page 2-57 changes

9.2.2. Multi-Office/Multi-Entity Projects

However, multi-office/entity projects can represent a significant challenge to the materials management team in defining system, **security**, and communication requirements

Page 2-60 changes

9.3.1 System Features and Capabilities

Sufficient operating flexibility to allow:

- Controlled frequency of reporting.
- Use of exception or alert reporting instead of full status reports.
- Use of CRTs or PCs at any location for status rather than print-outs.
- Reduction or elimination of interfaces when file updates are not required.
- Selective elimination of entire systems and files when the need no longer exists or can be handled manually at lower cost.
- **User privileges and authority limits.**

Page 2-62 changes

9.4 Planning and Systems Management

Because of the potential cost and needed control of integrated systems involving numerous project participants/personnel, the materials plan should include provisions to:

- Assign overall control for systems to a single individual who should be thoroughly familiar with the systems and the associated consequences/cost. **The system administrator should undergo a thorough background investigation.**

Page 2-64 changes

Scheduling the entire materials activity is essential to meeting the project timetable. Materials schedules are as critical as those of engineering and construction and span all phases of the project, from defining and approving the requirements to purchasing, supplier lead time, logistics, **security**, and site management.

Chapter 3: Organization and Personnel

Page 3-15 changes

4.2 Field Project Organization Skills

4.2.1 Site Materials Manager

This position requires extensive skills in all phases of materials management, particularly in physical control of all field materials. Extensive experience and knowledge of a wide diversity of construction materials are necessary. Familiarity with home office engineering and materials management practices is a distinct plus. Also needed are skills in materials descriptions and classifications, advanced planning and scheduling, and receiving, inspection, warehousing, issuing, shipping, **and securing** of required materials.

Chapter 4: Computer Systems

Page 4-14 changes

6.0 Computer Systems

Whichever method is selected, the portability **and security** of the data is important. The database should be ODBC (Open DataBase Connectivity) compliant, which enables exporting the database to another system and receiving inputs from other systems without a large amount of cost and effort.

Page 4-16 changes

9.0 Future Trends

Likely more systems are tied in some way to CAD systems. Certainly over the last 10 years there has been a growth in electronic communication between buyers and suppliers via e-mail and the Internet. **At the same time, this has created additional security vulnerabilities that should be addressed.**

Page 4-17 changes

The ability to track information globally within a company will be improved. More work will be performed, not in the office, not at home, but at project sites. **The growth of wireless communications has introduced additional security concerns.**

Chapter 5: Special Construction Techniques

Page 5-1 changes

This chapter will address the special materials management techniques and controls needed to realize maximum benefits from these construction techniques and to manage the increased complexities and special considerations (**e.g. labor availability, security, etc.**) that are a part of these techniques.

Page 5-6 changes

3.4 Other Factors

Other project factors that must be taken into account in preparing the SCT utilization study include:

- **Security** requirements for fabrication and transportation.

Page 5-26 changes

5.0 Summary and Conclusion

While the use of modular techniques is not always the answer to addressing these concerns, given the right circumstances, these benefits will result for the owner. Each project must evaluate the constraints (**e.g. labor availability, security, etc.**) that impact the construction to determine whether a fully prefabricated approach, partially prefabricated approach, or a fully conventional stick-built approach is the proper way to construct a given facility.

Chapter 6: Materials Requirements Planning

Page 6-12 changes

4.4 Acquisition Strategies

For fast-track projects, where construction begins before engineering is complete, bulk materials items will need to be on hand before total project quantities are known. Often lead times for materials preclude the luxury of developing takeoff quantities in time to purchase and deliver to meet the construction schedule. In this case, an "initial bulk buy" will have to be made from estimated quantities. This effort, if not supported with later, frequent and automatic quantity checks, can result in excessive surpluses or shortages. Factors that must be considered in determining "initial bulk buy" quantities include:

- Likelihood of engineering change
- Materials availability
- Transportation constraints
- **Security consideration**

Page 6-22 changes

4.8.4 Logistics Strategy

Consideration of transportation capabilities to, from, and on-site, including duration, equipment availability, **security requirements**, facilities, traffic control, expediting and cost.

Chapter 7: Purchasing

Page 7-33 changes

36. Do you have a substance abuse program?

If yes, does it include the following?

Preplacement Testing

Random Testing

Testing for Cause

DOT Testing

Do you conduct background Investigation on all of your employees assigned to our site?

Page 7-38 changes

Responsiveness

Supplier personnel (sales and technical) are professional and proficient
Supplier personnel are enthusiastic; are prompt; offer opportunities for improvement and move quickly to resolve problems
Cooperative with quality and safety surveys
Complies with security policies and procedures

Chapter 8: Expediting

Page 8-23 changes

XII. Packaging and Shipment

A. Determine Scope and Requirements

1. Final inspection or testing complete
2. Documentation
 - a. Packing lists
 - b. Manifests
3. Packing
 - a. Packing by supplier or third party
 - b. Special packing requirements or specifications
 - c. Special protective or preservative requirements
4. Transportation
 - a. FOB terms of order
 - b. Selection of carrier
 - c. Coordination with buyer's traffic department
 - d. Special loads — heavy lifts, oversize, **security**

Page 8-24 changes

2. Nature of problem

- a. Refusal to perform
- b. Dispute regarding terms of order
- c. Supplier error — misplaced order, over-booked line
- d. Lack of information
- e. Delay from backlog
- q. **Security**

B. Solution Analysis — Involved Parties

1. Internal
 - a. Engineering

- b. Scheduling
- c. Purchasing
- d. Traffic
- e. QA/QC
- f. Legal
- g. Client
- h. Corporate Management
- i. **Security**

Page 8-42 changes

8.6 Expediting Alert Notice

This form typically includes summary information regarding the order and its current status as well as a description of the delay or problem and the items affected. The form is circulated to appropriate project sectors and is then returned to the expeditor with instructions indicating what corrective actions, if any, are required or authorized. The form may also be used to alert engineering and purchasing personnel of current or upcoming problems with a particular supplier or supplier's facility that might affect pending decisions of further order awards. This may include conditions such as labor strikes or slowdowns, shop overloads, equipment failures, natural disasters, scheduled shutdowns, **security incidents**, and others.

Chapter 9: Quality Assurance and Quality Control

Page 9-4 changes

3.0 Quality Program Planning (Quality Assurance)

Unique inspection and test requirements are developed for each major engineered item. These plans should be developed by or in conjunction with the design engineer and take into consideration such factors as:

- Item complexity
- Item capital costs
- Cost of failure in production
- Safety in production
- **Security**
- Schedule

Page 9-5 changes

4.0 Supplier Selection and Relationship

Nonconformances should be detailed as to source or cause such as fabrication, test failure, improper or inadequate documentation, marking, packaging, or general workmanship. Ratings should also include other factors, such as schedule compliance, labor relations, cooperation, safety, **security**, technical capability, and service. For engineered equipment specified using performance criteria, the process of prequalifying bidders may include a requirement that potential suppliers submit to the owner or contractor a copy of their own quality control procedures for review and acceptance.

Chapter 10: Transportation and Logistics

Page 10-2 changes

The volume and nature of the freight, special logistics considerations, the jobsite location, special aspects of the project schedule, project funding, trade restrictions, government rules, **security issues**, and client requirements all are among the project-specific factors which must be researched and addressed in the T&L plan.

Page 10-4 changes

2.1.1 Formal Contracts and Alliance Agreements

Some of the standard points to consider when drafting a transportation contract are:

- A severability provision (specifying that even if one clause is held invalid, the other terms of the agreement will remain in effect).
- The carrier's transit, demurrage, and terminal privileges (applies to rail contracts only).
- **Security performance requirements.**

Page 10-5 changes

The buyer's motivation for entering into an alliance agreement for transportation or logistics services may include:

- Reduction in duplicated activities.
- Reduction in staffing required.
- Greater control of confidential information **and increased overall security.**

Page 10-19 changes

3.2 Transportation and Logistics Plan

The plan should detail how project-specific issues will be handled including the following as applicable:

Unsatisfactory, over, short, or damaged reports and claims

- Small shipments
- Payment for transportation services
- Hazardous and restricted materials
- Short shelf life materials
- Bonds
- **Security requirements**

Page 10-20 changes

As an example, the following is a listing of many of the elements usually addressed in a logistics planning effort for the more complex overseas projects or for projects with significant imports:

- Rail and Truck Equipment (all types) — Availability, freight cost for principal commodities, transit schedules, and intermediate control points.
- Destination Conditions — Conditions at destination (jobsite) pertaining to operations of the delivering carriers and the shipping agents.
- **Security situation at origin, during transit, and at destination**

Page 10-21 changes

3.3.2 Details of the Survey

In most cases it is wise to arrange for the routes to be driven and other facilities visited to visually determine actual conditions. Traditional constraints such as overhead obstructions, tunnels, sharp curves, weight restricted bridges, severe inclines, inclement weather, **local security conditions**, and governmental requirements must all be investigated prior to determining the maximum envelope for design criteria for large plant equipment such as vessels, heat exchangers, skidded equipment, or modules.

Page 10-22 changes

3.3.3 Information Requirements

The logistics survey should uncover any and all restrictions to transportation from all sources of supply to the jobsite. As a guide, the following is a listing of considerations/inputs, which should be covered in the route survey report:

- Identification of specific routes with charts/maps plus indications of mileage to destination.
- **Identification of security vulnerabilities and protective measures required along route.**

Page 10-24 changes

3.4.1 Coordination with Local Authorities

In addition to the constraints discussed in section 3.3 above, care should be taken to consult local governmental authorities for initial transportation plans to ensure that those plans do not adversely affect local transportation patterns or violate local ordinances restricting traffic. **Ensure that local authorities are consulted with regarding planned security requirements.**

3.4.2 Personnel Transportation

Remote site personnel transportation can present unique concerns to the transportation/logistics personnel. Alternatives of chartered air and dedicated bus service should be considered, **as well as their security implication**

Page 10-33 changes

4.2 Personnel Requirements and Experience

It can sometimes be difficult to find personnel with well-rounded knowledge of these various areas of transportation and logistics expertise. The basic functions performed by these specialists include:

- Coordinating air shipment; ensuring that technical documentation and material shipments are properly packed, documented, and marked per the project's requirements.
- **Coordinate security requirements.**
- Coordinating both domestic and international household goods shipments.

Page 10-40 changes

4.7.1 Export Preparation

Preplanning packaging and preservation requirements are essential. Concern for equipment protection has increased because:

- Storage conditions, installation dates, and startup times often are not known when equipment is purchased.
- Logistical difficulties may require unique packing and crating methods that are not widely used.
- **Local/regional security threats.**

Page 10-52 changes

5.0 Summary and Conclusions

Each country's customs requirements are unique with potentially significant duties, taxes, fines, and lengthy delays, which must be considered in the planning efforts. **Increasingly, transportation security must be considered in planning and risk analysis.**

Chapter 11: Site Materials Management

Page 11-2 changes

1.0 Introduction

Effective management of materials at the construction site can contribute significantly to the success of a project. To be effective, however, the site functions and activities must be an integral part of an overall materials management program that is fully supported by project management, site management, and craft personnel. Site materials management extends beyond the activities of receiving, storing, and issuing materials. The identification, requisitioning, purchasing, and expediting of all materials not procured by the home office comprise a significant part of the site materials effort. It is also affected by other elements of project management, including engineering, procurement, expediting, **security**, and inspection

Page 11-19 changes

5.2 Warehouse Facilities and Storage

Inside Storage Area — Inside warehouse storage is provided for specific items. Areas are arranged to receive, store, issue, and inventory materials and supplies. Shelving, storage bins, and pallet racks are conformed to the needs of each warehouse section for the materials to be stored. Inside storage areas should be established for:

- Small bulk items (e.g., bolts, electrical fittings, engineered components, expendable supplies, instrumentation, nuts, small bore valves and fittings, and spare parts). These items are grouped by type and size and then stored in individual bins identified by description and size.
- Electrical and/or instrument panels.
- Fragile items, instruments, lighting fixtures.
- Items that require climate control (e.g., instruments, welding supplies).
- **High security items.**

Issue Area — An issue counter provides a central point inside the warehouse where craft personnel can drop off warehouse requisitions and pick up issued materials.

Ideally, the layout and design of laydown areas and warehouse space should be completed prior to site mobilization. Allocating and scheduling the use of laydown space can be a significant coordination effort, especially when multiple contractors are involved. **In both cases, adequate security measures (e.g., fencing, security lighting, access control) should be employed as required.**

Page 11-23 changes

Truck Deliveries — Incoming truck deliveries are directed to the warehouse for unloading with the following guidelines:

- Must comply with security policies and procedures.

Page 11-24 changes

Construction Equipment — Construction equipment and vehicles require documented, incoming inspection by a representative from the construction site's equipment department and warehouse personnel. Damaged items are documented on shipping papers and inspection reports even though the equipment's operation may not be affected (e.g., dents in a door). This inspection is repeated when the equipment is released from the project. Rental status logs provide accurate records of incoming and outgoing construction equipment. Logs should indicate such

items as date received, purchase order number, assigned equipment number, description of equipment, make and model, supplier renting/leasing the equipment, and date released. **Stringent controls should be in place to prevent misuse.**

Fuel — Provide an above ground storage tank for unleaded gasoline and diesel. Tanks should have a sight gauge or an access hole in the top of the tanks to allow measuring. Tanks should also be equipped with a metered pump (complete with lock) to record disbursements. **Stringent controls should be in place to prevent misuse.**

Chapter 12: International Project Materials Management

Page 12-2 changes

2.2 Surveys

The international project planning effort will be enhanced considerably by early and timely surveys within the host country to gather critical information essential to the development of a well thought-out materials plan. This is particularly true if the contractor and owner do not have recent experience in the host country and/or locale of the project jobsite. Typically, these surveys should address the following areas:

- **Conduct SVA.**
- Potential shipping facilities (ports), storage, and transportation routes (highway and rail) to the jobsite.

Page 12-5 changes

2.6 Project Camps

Detailed planning is necessary to ensure proper quarters and supplies. Food and related goods can be a particular concern considering import regulations, availability of quality food stuffs, and the potential difficulties of transporting perishable goods to the site(s), while also recognizing the local culture and habits of those who may be employed to support the project execution effort. Planners (and the implementing organization) must always be aware that a lack of any item can have a devastating effect on morale and productivity. **Proactive measures to secure the camp may be required in certain locations.**

Page 12-25 changes

8.3 Organization

On the other hand, if a project is large and remotely located and project organization and operations need to be self-sufficient, then the activities of the logistics section could include all or part of the following:

In-country transportation via owned or leased equipment

- Scheduling and arranging third-country shipments
- Supervision of trans-shipment points, staging areas, offshore packing and preservation, loadings, and import documentation
- **Coordination/procurement of security services**

Page 12-28 changes

9.0 Warehousing

When constructed, the permanent warehouse facilities should be located with good access to equipment and workshops and also to the major project work areas. Depending on the nature of the project, warehousing may need to establish special yards or remote storage areas to provide for large or bulk items such as fuels, explosives, asphalt, paints, chemicals, construction gases, cement, steel, fabricated items, building materials, pipe, fencing, cable, tires, and scrap/salvage materials. **Security procedures to protect these items should also be considered.**

Page 12-30 changes

9.5 Loss of Inventory

Theft and pilferage are potentially significant problems in some UD/D countries. When required, preventive measures should be administered intensely and relentlessly. **Continuous or periodic physical inventory checks and security procedures are therefore among the most important warehousing activities on remote projects.**

Page 12-32 changes

11.0 Summary and Conclusions

International materials management has many unusual (sometimes unique) complications that can have a severe impact on cost, schedule, and quality. In

particular, contractors and owners with overseas projects should plan for potential delays in licensing, customs, and transportation. They also should be prepared to deal with different labor laws and local materials pricing and quality standards. To the greatest extent possible, audit functions should be included in all areas of materials management. **Security challenges presented by international projects may be different from those experienced domestically and may require additional efforts and assets to successfully manage those threats.**

Chapter 13: Materials Management for Commercial and Small Projects

Page 13-2 changes

2.0 Planning

Other examples of project constraints that have a direct impact on the contractor's materials management plan include:

- Restricted access to the site
- Lack of adequate laydown area or warehouse space
- Extended purchasing approval cycle
- Accelerated schedules
- **Security requirements**

Page 13-3 changes

2.1 Owner's Requirements (Items to be Identified)

- Materials specifications
- Project purchasing procedures
- Project supplier list
- Materials requirements (i.e., detailed information on what materials have been purchased (owner-provided) and what falls into "Scope of Work")
- **Security requirements**

Chapter 14: Guidelines for Evaluating A Contractor's Materials Management System

Page 14-3 changes

1.0 General Project Characteristics

A. Facility type, size, and geographical location

- B. Scope of contractor's services with respect to design, procurement, and construction
- C. Contract type (cost-reimbursable and any incentive clauses vs. lump sum)
- D. Schedule constraints, budget constraints, jobsite environmental constraints (need for modularization), union constraints, **security constraints**, and governmental constraints

Page 14-9 changes

- 4.0 Computer System
 - A. General capabilities
 - Materials categories managed by the computer system
 - Materials management functions (2.0 A above) performed by the computer system
 - Batch or on-line operation, frequency of updates and types of reports
 - System limitations (maximum number of file records, maximum number of requisition or PO line items)
 - Interface plan
 - **Configurable permissions and data access controls**

Page 14-14 changes

- 9. Describe the general system hardware and software platforms.
Configurable permissions and data access controls

Appendix B: Materials Plan Outline

Page B-1 changes

- 1.0 Purpose
- 2.0 Project Definition
 - 2.1 General
 - Title, Type, and Size Facility
 - General Location of Facilities
 - Security assessment**

Appendix C: Glossary

Add definitions of:
Security
SVA

Appendix I: Job Site Security Guidelines

A Job Site Security sub-team to the Practice Development Team developed the following guidelines.

JOB SITE SECURITY ELEMENTS

Elements are dependent upon size and complexity of project and operating environment. "Inside the Fence Line" projects will typically incorporate existing security measures, but require in-depth consultation between Owner and Contractor Security Rep's. These types of projects provide access to existing operating areas, but generally have more mature security systems.

Security considerations on "Greenfield" projects will typically be more Contractor driven. "Greenfield" projects can be less of concern regarding international terrorist acts but have unique loss prevention opportunities.

Basic elements are used in consideration of the "Anticipate, Deter, Detect, Delay, Respond, and Mitigate" doctrine as it applies to Security. This applies to internal and external threats to the site. Threats can include destruction, sabotage, theft, or other related activities. It is assumed that local law enforcement and federal agencies will be the primary source of intelligence and the primary responder to armed intrusions.

- Threat Level Response Guidance
 - Provide guidelines that correspond to Department of Homeland Security threat levels.
- Responsible Person for Security
 - Owner and Contractor Corporate Representation
 - Frequency of Site Inspection and visits.
 - Dedicated (assigned responsibility) Site Security Supervisor reporting through Construction Manager. Coordinates activities with Corporate Director of Security.
- Perimeter Control
 - Fencing Considerations
 - Intrusion Detection vs. Non-Intrusion Detection
 - Gate Configuration
 - Sized for emergency vehicle access
 - Multiple gates

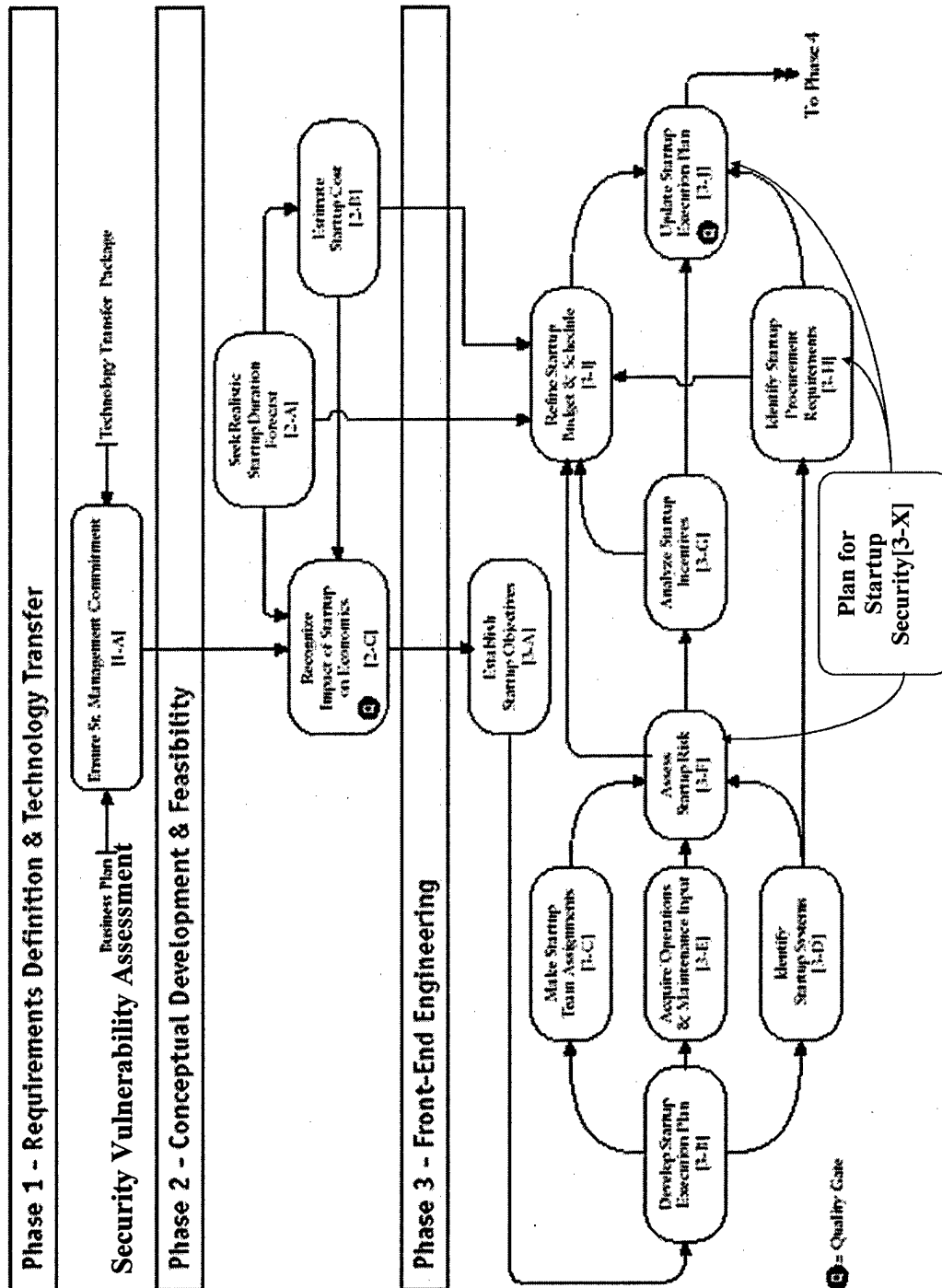
- Access Control
 - Search Policy Posted
 - Accountability
 - Vehicle Control
 - Vehicle Tagging Procedures
 - Visitors
 - Employees
 - Deliveries
 - Material/Equipment Removal
 - Mustering Capability
 - Access Control Badge Policy
 - Photo identification badge system (Prox/Mag Card)
 - Badge Control Issuance/Retrieval Policy
- Employee Screening Protocols
 - Human Resource involvement in Application Process.
 - Criminal History Background Screening
 - Fair Credit Reporting Act Issues
- Cost/Budget Considerations in comparison to Project planning.
- Material Controls
 - Scrap & Salvage Procedures
 - Inventory procedures of tools/materials
 - Unique security considerations of materials/products?
- Key & Lock Control
 - Proprietary System
- Guard Service Selection
 - Armed vs. Unarmed
 - Written Post Orders
 - Training Standards & Expectations
 - Indemnity & Bonding
- Lighting
 - Perimeter
 - Gate
- Site Specific Construction Site Security Plan vs. boilerplate
 - Ensure Security Plan coordinated with Industrial Relations (IR) plan
- Emergency Action Planning
 - Weather (Flood, Tornado, Hurricane, etc...)
 - Explosion, Fire
 - Chemical Release
 - Bomb Threat
- Communication Systems

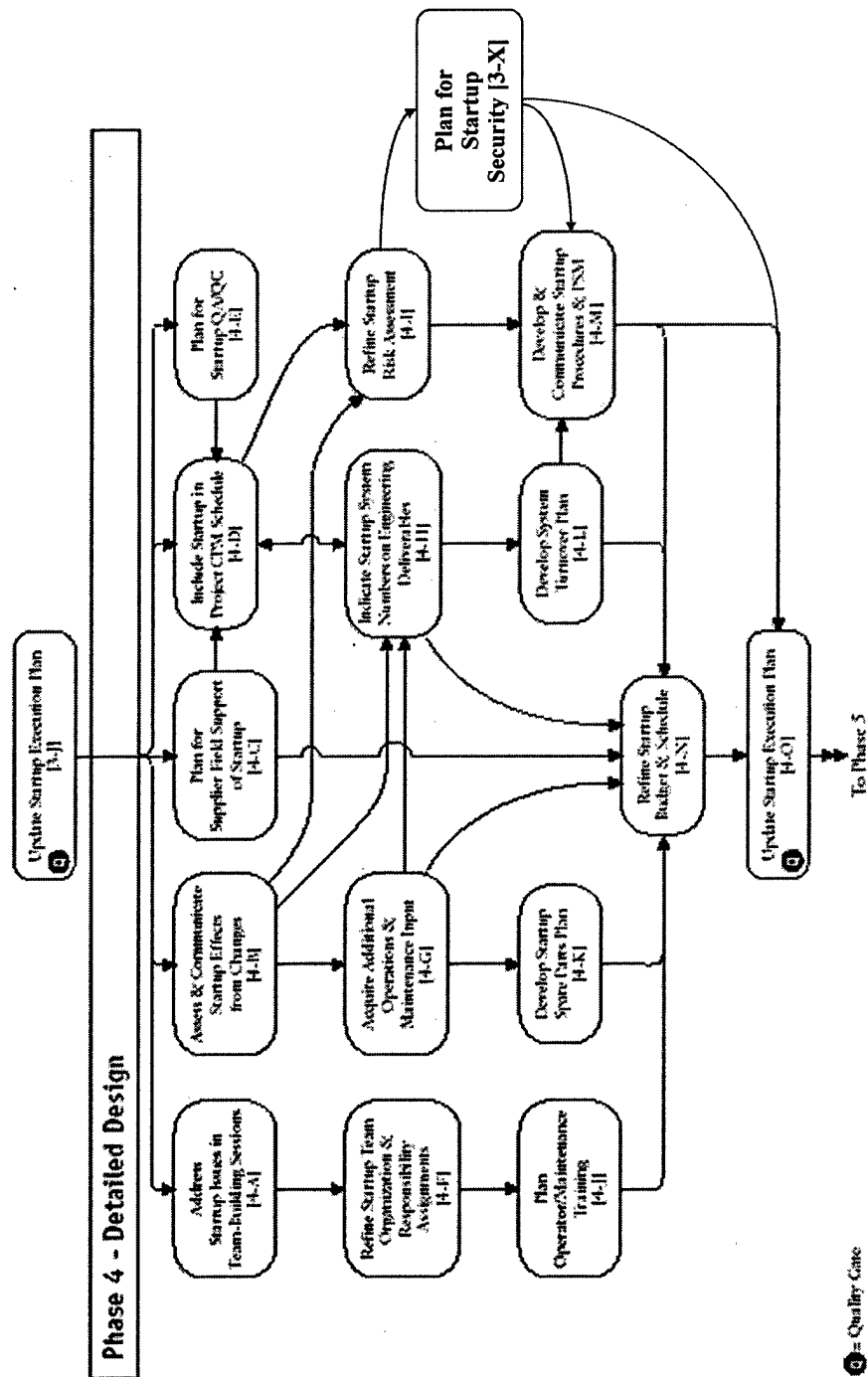
- Phone System Capabilities (Caller ID capable)
 - Radios
 - Cellular
- Cyber/IT
 - Network Systems
 - Wireless Applications (Security of)
- Security Training/Education (General Employee)
 - Security Incident Reporting Procedures & Documentation
 - Drug/Alcohol Policy (Can be contract driven)
 - Workplace Violence Policy
 - Contraband/Search Policy
 - No Firearms on Site (Including Parking areas) Policy
 - Ethics Policy & Hotline
- Proprietary Information Security
 - Document Classification System
 - Document Destruction (shredding on-site/offsite)
 - Document Retention Policy
- Parking Areas
 - Shared or Dedicated
 - Secured vs. Non-Secured
- Electronic Security Systems
 - Alarm Systems
 - Local vs. Central Monitoring
 - CCTV Systems
- Security Vulnerability Assessments Results & Considerations
 - Was an SVA completed and are the results available?
- Ethics Policy & Hotline
- Local Law Enforcement Issues & Consultation
 - Intelligence/Information exchange
- Security Incident Reporting Procedures & Documentation
 - Security Post Orders
 - Employee role in reporting security concerns/incidents.
- Cleaning Staff Selection and Screening
- Heavy Equipment
 - Theft Issues
 - Sabotage Issues
 - Accountability Issues (Usage)
- Expat Issues (International Projects)
 - Housing/Compounds Security
 - Transportation Security
 - Contingency Plan in case of emergency

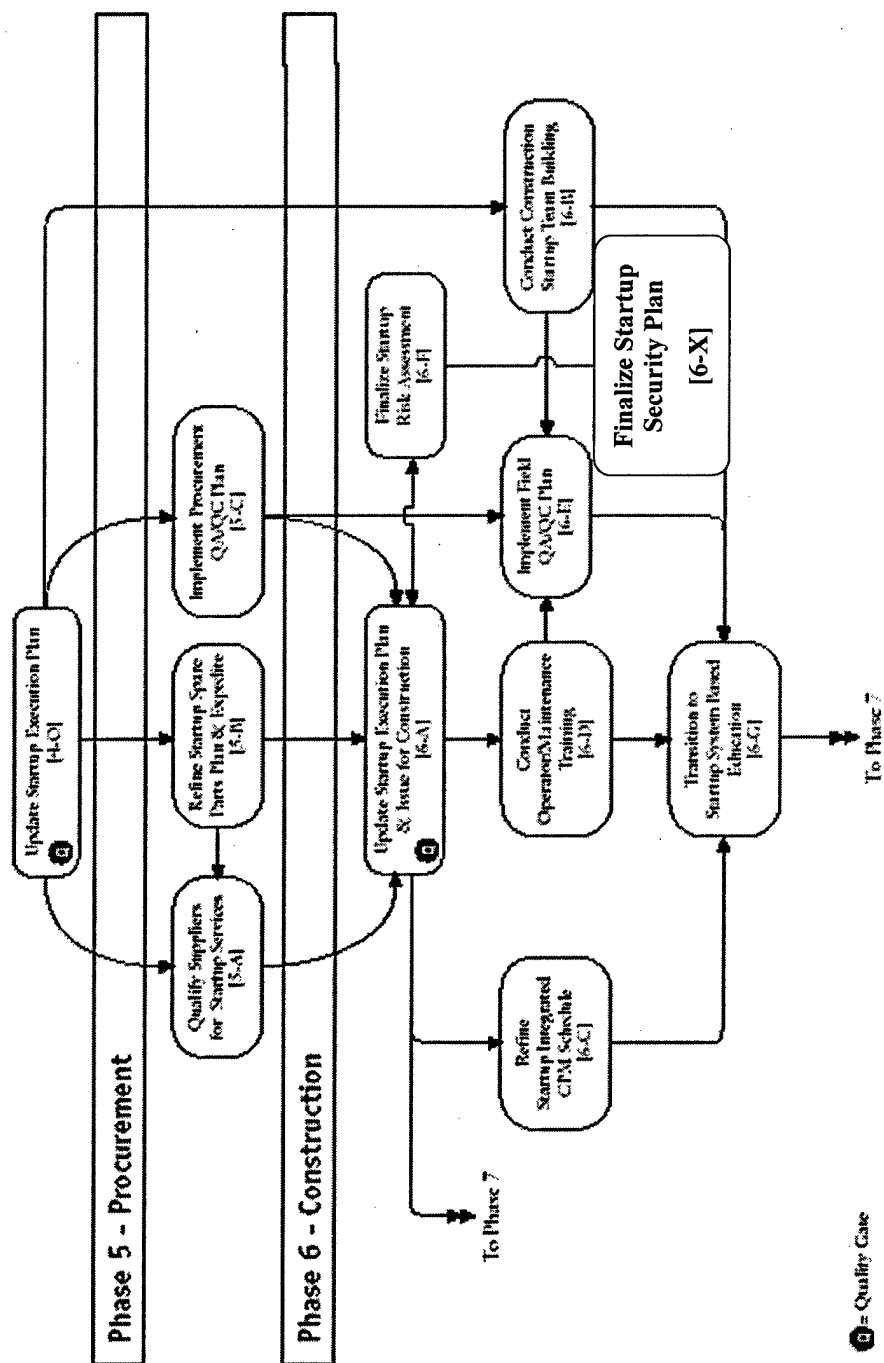
Appendix J: Planning for Startup Updates

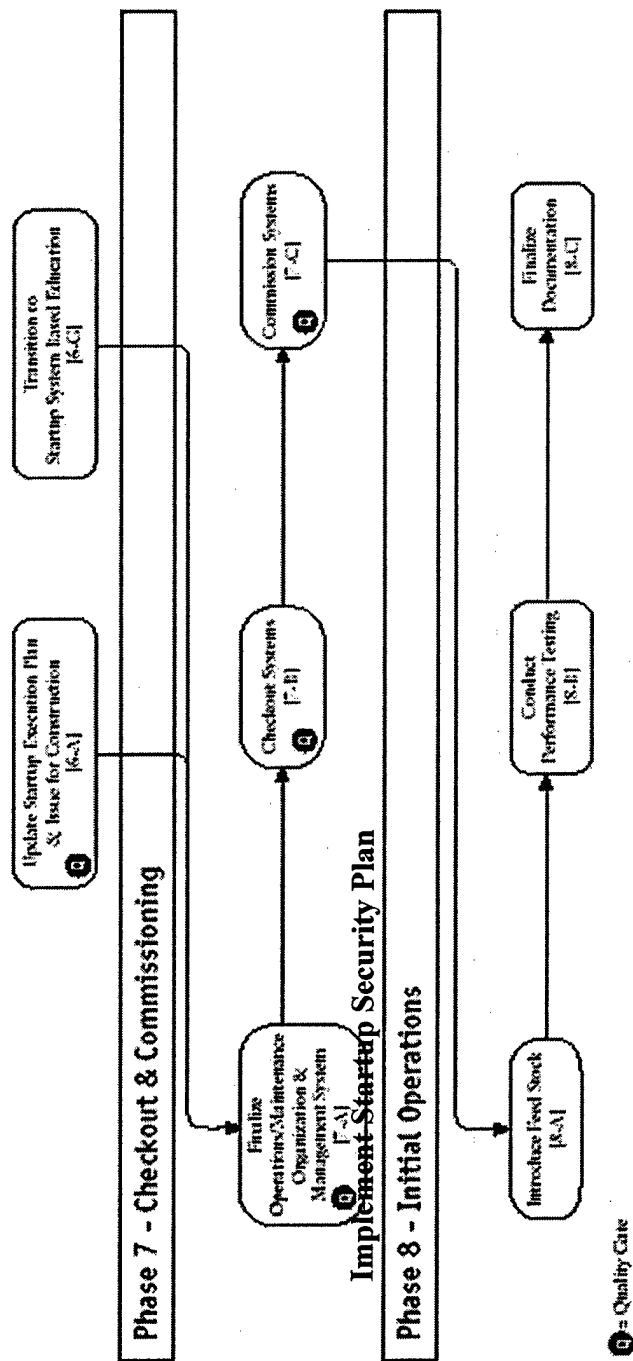
The following updates were made to CII Implementation Resource 121-2

“Planning for Startup” (1998) Changes are indicated in bold.









Page 8 changes

Plant Operations & Maintenance Management:

- Plant operations and maintenance personnel are responsible for many important startup planning activities in front-end engineering and detailed design phases, **including input into startup security planning.**

Page 22 changes

2-B: Estimate Startup Costs

G. Basic Steps:

1. Ensure that the best possible basis documentation is used.
2. Consider or include the following in the startup cost estimate:
 - A well-defined basis for beginning and ending points, such that meaningful cost estimates can be included for startup operations.
 - Pre-startup costs for startup planning, **security** and training.
 - Factors such as work-hours, raw material, and auxiliary material.

Page 23 changes

2-C: Recognize the Impact of Startup on Project Economics

G. Basic Steps:

1. The startup team must be proficient with the chosen technology in order to successfully deal with the emerging problems associated with starting up new technology.
2. Project venture objectives must be clearly understood for optimal project and startup planning so that venture economics can be realized.
3. Conduct an economic analysis of startup costs versus early/on-time/late product delivery. In conducting sensitivity analyses of "what-if" scenarios,

take the following questions into consideration: Is the product in short supply? How much product can be sold in the first year? What are the lost profits for each day the plant is not on-stream with salable product? What is the capital versus profit trade-off? Should extra capital be expended to ensure on-time product with adequate quality? Has the project team focused on optimizing engineering, construction, and startup in a global sense vs. suboptimization? **Have startup security costs been adequately resourced?**

Tool 2-B: Example of Startup Cost Breakdown Structure (page 1 of 4)

Item #	Item	Planning effort (Work - ours)	Implementation effort (Work - ours)	Material Cost	Services Contract Cost
1	Requirements Definition & Technology Transfer Engineering efforts Phase Subtotal				
2	Conceptual Development & Feasibility Engineering efforts				
3	Manufacturing/Operations efforts				
4	Maintenance efforts				
5	Outside services: labs, consultants, certifications, security				
	Phase Subtotal				
6	Front-End Engineering Engineering efforts				
7	Manufacturing/Operations efforts				
8	Maintenance efforts				
9	Outside services: labs, consultants, certifications				
	Phase Subtotal				

Tool 2-B: Example of Startup Cost Breakdown Structure (page 2 of 4)

Item #	Item	Planning effort (Work-Hours)	Implementation effort (Work-Hours)	Material Cost	Services Contract Cost
11	Detailed Design				
12	Manufacturing/Operations efforts				
13	Maintenance efforts				
14	Outside services: labs, consultants, certifications, security				
	Training program development				
	Phase Subtotal				
15	Procurement				
16	Engineering efforts				
17	Construction efforts				
18	Manufacturing/Operations efforts				
19	Maintenance efforts				
20	Outside services: suppliers, labs, consultants, certifications				
21	Training program development				
22	Materials & equipment expense				
23	Utilities				
	Feedstock, catalyst, raw material, product handling				
	Phase Subtotal				

Tool 2-B: Example of Startup Cost Breakdown Structure (page 3 of 4)

Item #	Item	Planning effort (Work-Hours)	Implementation effort (Work-Hours)	Material Cost	Services Contract Cost
24	Construction				
25	Engineering efforts				
26	Construction efforts				
27	Manufacturing/Operations efforts				
28	Maintenance efforts				
29	Outside services: suppliers, labs, consultants, certifications				
30	Training program development and implementation				
31	Materials & equipment expense				
	Utilities				
	Phase Subtotal				
32	Check-out & Commissioning				
33	Engineering efforts				
34	Construction efforts				
35	Manufacturing/Operations efforts				
36	Maintenance efforts				
37	Outside services: suppliers, labs, consultants, certifications, security				
	Training program				

Tool 2-B: Example of Startup Cost Breakdown Structure (page 4 of 4)

Item #	Item	Planning effort (Work-Hours)	Implementation effort (Work-Hours)	Material Cost	Services Contract Cost
	Check-out & Commissioning (continued)				
38	Material & equipment expense				
39	Utilities				
40	Feedstock, catalyst, raw material, product handling				
	Phase Subtotal				
	Initial Operations				
41	Engineering efforts				
42	Construction efforts				
43	Manufacturing/Operations efforts				
44	Maintenance efforts				
45	Outside services: suppliers, labs, consultants, certifications, security				
46	Material & equipment expense				
47	Utilities				
48	Feedstock, catalyst, raw material, product handling				
	Phase Subtotal				

Tool 2-C: Startup Financial Risk Assessment Checklist (page 2 of 2)

#	Risk Issues	Risk Assessment				Not Applicable	Comments
		Low	Med.	High	Uncertain		
D	Schedule Issues						
	Level of Project Scope Definition						
	Realistic Milestone Dates						
	Status of Long Lead Procurement						
	Permitting Delay Impacts						
	Effect of Incentives						
	Level of Liquidated Damages						
	Labor Probs./Coll. Bargaining Agreement						
	Other:						
E	Funding Issues						
	Realistic Budget						
	Realistic Contingency & Eff. Mgmt.						
	Expected Labor Productivity						
	Other:						
F	Existing Plant/Site						
	Adequacy of Utilities						
	Accessibility/Congestion						
	Impact to Ongoing Operations						
	Other:						
G	Miscellaneous						
	Handling of Hazardous Material						
	Off-Spec Product Disposal						
	Quality of Startup Planning						
	Inherent Safety Hazards						
	Other: security						

Note: This checklist is not all-inclusive, but is intended primarily to stimulate discussion.

Page 31 changes

3-A: Establish Startup Objectives

I. Challenges to Successful Implementation:

- Lack of understanding of startup objectives and their importance on the part of the business unit.
- Misalignment of startup objectives between project management and business unit personnel.
- **Security is sometimes overlooked as a startup objective.**

Page 32 changes

3-B: Develop the Startup Execution Plan

E. Responsibility: Manufacturing Operations Representative, Startup Manufacturing Operations Representative, Project Team

Accountability: Owner Project Manager

Consult: Contractor Project Manager, Planner/Scheduler, **Security Manager**

Inform: Plant Manager

F. Quality Gate/Sequencing Constraints: This activity is not a quality gate, but should occur early in Front-End Engineering.

G. Basic Steps:

1. Gather key contributors to the Startup Execution Plan and discuss contents and drafting responsibilities. The Startup Plan should include a detailed listing of all startup objectives (see activity 3-A). The Startup Plan should establish the criteria for the following: startup philosophy; commitment to startup quality gates; identification of startup systems on engineering documents; identification of needed resources for startup execution and operations; startup responsibilities (including those of suppliers and operators); conceptual schedule, addressing processes, areas, utilities, etc.; operator training needs; startup raw material needs; identification of startup risks; plans for check-out/commissioning, **security systems and transitions**, and initial operations. Considerations in developing the startup philosophy include product priorities, schedule phases and sequencing, production

ramp-up curve, and integration with shutdowns, along with other schedule "drivers."

Page 33 changes

3-C: Make Startup Team Assignments

G. Basic Steps:

1. Consult the Startup Execution Plan, refining the draft organization chart. The organization chart must be compatible with the RACI table.
2. Put names on the organization chart, considering areas requiring special expertise. Consider having the **Safety Manager/Security Manager** and the QA/QC Manager report to both the Construction Manager and the Startup Manager.
3. Communicate the assignments.

Page 34 changes

3-D: Identify Startup Systems

G. Basic Steps:

1. Consult the Startup Execution Plan and use it as a basis for this activity.
2. Recognize all contracting strategy limitations of the project.
3. Use P&IDs to breakdown the plant into startup systems. Get early input from operations, process design, controls, construction, and maintenance.
4. Indicate startup system boundaries on the P&IDs.
5. Conduct crosschecks: will operations and control systems support the startup logic? Will the construction sequence support the startup logic? Will environmental testing criteria **and security plan** support the startup logic? Will available owner staffing support the startup logic?
6. Establish the listing of startup systems.

Page 35 changes

3-E: Acquire Operations & Maintenance Input

G. Basic Steps:

1. Conduct O&M input meetings, addressing the following issues:
 - Specific maintenance requirements: preferred suppliers, spares, access needed, and supplier data requirements.
 - Specific operation requirements: process control, operator preferences, and access requirements.
 - Specific checkout requirements: safety, acceptance criteria, staffing, interlocks, hazards, communication, and lockouts.
 - Specific startup requirements: system sequence, timing, utilities needed, safety procedures, **security provision**, and environmental requirements.

Page 36 changes

3-F: Assess Startup Risks

E. Responsibility: Manufacturing Operations Representative, Startup Manager

Accountability: Owner Project Manager

Consult: Contractor Project Manager, Planner/Scheduler, Process Licensor,
Security Manager

Inform: Plant Manager

G. Basic Steps:

1. Consult the Startup Execution Plan, **Security Vulnerability Assessment, and lessons learned to date.**
2. Review startup lessons learned to date.
3. Identify risks associated with the process technology **and process hazards.**
4. Identify risks associated with the controls automation.

5. Address degrees of redundancy and planned levels of maintenance.
6. Identify risks associated with environmental **and security** concerns.

Page 38 changes

3-H: Identify Startup Procurement Requirements

G. Basic Steps:

1. Prepare a list of startup items than need to be procured and integrate startup procurement with overall procurement activities.
2. Establish procurement responsibilities (owner, engineer, etc.).
3. Identify long lead **and security sensitive** items ~~(to ensure timely deliveries and thereby avoid schedule impacts on startup dates)~~. Establish if early release of funds will be required.

Page 40 changes

3-J: Update the Startup Execution Plan

G. Basic Steps:

1. Build upon and expand the previously developed Startup Execution Plan (activity 3-B). Incorporate the most recent startup budget and schedule (activity 3-I), startup procurement requirements (activity 3-H), startup incentive systems (activity 3-G), assessment of startup risks (activity 3-F), **plan for startup security (activity 3-X)**, listing of startup systems (activity 3-D), startup team assignments (activity 3-C), and any other salient information.
2. Reevaluate the use and effectiveness of startup quality gates.

Page 41 changes

Tool 3-A: Listing of Typical Startup Objectives (page 1 of 8)

9. Security Assurance **Security is assured during all phases of startup, including transition from construction to an operations phase.**

Page 46 changes

Tool 3-A: Listing of Typical Startup Objectives (page 7 of 8)

Table 3-A-4. Example Computation of Criteria Importance Weightings

Success Criterion	Assigned Importance	Importance Score	% Contribution to Total Score	Importance Weighting
Product Quality	Above average	4	12.5	0.125
Product Quantity	Above average	4	12.5	0.125
Schedule Performance	Above average	4	12.5	0.125
Safety Performance	Most important	5	15.6	0.156
Environmental Performance	Most important	5	15.6	0.156
Operations Team Performance	Average	3	9.4	0.094
Impact to Operations	Above average	4	12.5	0.125
Security Assurance Level of Effort	Above Average	4	REWEIGHT	ALL SCORES
	Average	3	9.4	0.094
Total		32	100	1.000

Page 50 changes

Tool 3-B-2: Sample Table of Contents for the Startup Execution Plan

8 **Startup Risk/Security Management**

Page 52 changes

Startup Quality Gate 3J:

At this quality gate, all startup activities to be accomplished during Phase 3 (Front-End Engineering) are subject for review. This is the most important quality gate because as the project enters the detailed design phase, changes become increasingly more expensive and detrimental to schedule adherence.

Critical checkpoints are:

1. A startup manager has been appointed.
2. Startup objectives have been defined.
3. Startup systems have been identified for transfer to the engineering contractor.
4. A HAZOPS/Safety review **and security review** have been completed and startup risks have been identified.

Page 53 changes

Startup Quality Gate 6A:

This startup quality gate may not coincide with the overall project quality gate because it focuses on procurement requirements and startup team building and training. The major interfaces with construction are the field QA/QC program **and security program**. This startup quality gate review should take place early in the construction phase.

The following critical activities must be going on or must have been completed:

1. The supplier technical performance criteria, **security**, and QA/QC requirements are going out with each bid package.
2. Construction/startup team building has been implemented.
3. O/M (operations & maintenance) training is being implemented.

4. Field QA/QC and security plans ~~has~~ have been implemented based on startup systems.

Page 54 changes

Startup Quality Gate 7A:

This is a critical startup quality gate because it should give assurance to management that a knowledgeable startup team has been assembled and trained and is ready to commission the plant according to a detailed startup plan.

The following critical actions should have been completed:

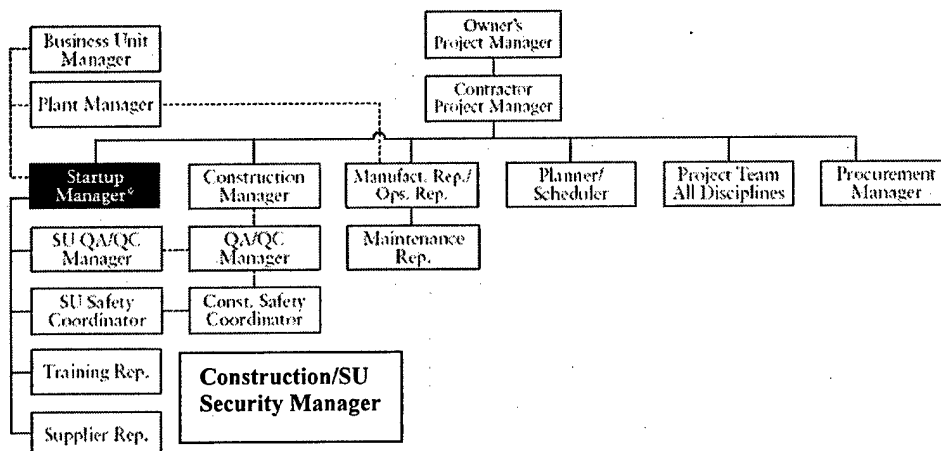
1. All named startup positions have been filled with qualified personnel.
2. All management procedures are in place.
3. "As designed" HAZOPS/Safety and security reviews ~~has~~ have been completed.

Startup Quality Gate 7C:

At this step the plant (system by system) must have been verified to be capable of safe and secure operation.

Page 55 changes

Tool 3-C-1: Sample Organizational Chart (page 1 of 2)



*The Startup Manager is an integral member of the Project Team and utilizes all members of the Project Team in planning for startup. This is a generic chart meant to emphasize the role of the Startup Manager. Obviously, such charts can vary by project and organization.

Page 70 changes

Tool 3-F: Startup Risk Assessment Checklist (page 2 of 3)

#	Risk Issues	Risk Assessment				Not Applicable	Comments
		Low	Med.	High	Uncertain		
C	Automation/Control Technology						
1	degree of definition						
2	previous in-house exper. & avail.						
3	proven process autom'n supplier package						
4	complexity/size						
5	system redundancies: controls						
6	process autom'n supply training & support						
7	simulation capability & effort						
8	other:						
D	Hazardous Materials/Processes						
1	hazardous chemicals						
2	explosive reactions						
3	inherent safety hazards						
4	likelihood of spills, emissions						
5	plant preparedness						
6	community preparedness						
7	RMP/PSM system adequacy & confidence						
8	health risk monitoring						
9	separation between processes						
10	emergency response plan						
11	other:						

Security plan adherence not all-inclusive, but is intended primarily to stimulate discussion.

Page 82 changes

4-C: Plan for Supplier Field Support of Startup

G. Basic Steps:

1. Understand and commit to the requirements of the existing change management system (thoroughly establish one if none exists!).
2. Add assessment of startup impacts to the change evaluation system, and whenever appropriate, involve startup expertise in the change management team.
3. Recognize that changes can cause delays, cost increases, unforeseen safety and health risks, **new security challenges**, loss of momentum, demotivated workers, and loss of organization and planning.

Page 89 changes

4-I: Refine Startup Risk Assessment

G. Basic Steps:

1. Use the updated Startup Execution Plan as the basis for this activity and revisit documented startup lessons-learned.
2. Conduct a formal risk analysis. Reassess risks associated with the process technology **and process hazards**, controls automation, redundancy, **security**, and environmental concerns. Involve a trained risk analysis facilitator as needed. Employ both checklists and formal risk analysis methods as appropriate (e.g., Monte Carlo analysis, event trees, scenario analysis, fault trees, etc.).

Page 93 changes

4-M: Develop and Communicate Startup Procedures and Process Safety Management

G. Basic Steps:

1. Use the Startup Execution Plan as the informational basis for this activity. Other key information documents for this activity include PFDs, P&IDs, logic diagrams, supplier technical data, Process Safety Management procedures (29CFR 1910), and previous startup procedures.
2. Review and discuss plant operational dynamics, including all foreseen operating conditions. Review and refine project safety procedures. **Review and refine project security procedures.** Complete the Process Hazards Analysis and develop procedures that address associated concerns.
3. Draft detailed startup procedures for review, refinement, and issuance.

H. Tools Needed/Provided:

Needed: company startup procedures; Process Safety Management checklist;
security plan

I. Challenges to Successful Implementation:

- Unavailability of qualified personnel at this stage for this activity
- Lack of field personnel with experience in Process Safety Management
- Inadequate or late supplier support of this activity
- Starting this step too late in the project
- Inadequate attention to safety **and security** issues as systems are turned over to operations

Page 96 changes

Tool 4-B: Checklist of Change Impacts on Startup

#	Change Evaluation Criteria	Change Impact					Comments/ Action
		None	Low	Med.	High	Uncertain	
A	Schedule Delays						
B	Authorization Reqrnts/Cost						
C	Safety and Health Risks						
D	Technical Basis for Change						
E	Environmental Compliance						
F	Product Quality						
G	Operability						
H	Maintainability						
I	Changes in Operating Procedures						
J	Operations/Maint. Training						
K	Mechanical/Control Integrity						
L	Loss of Project Momentum & Efficiency						
M	Project Team Demotivation & Tension						
N	Management Concerns						
O	Organization and Planning						

Page 114 changes

Tool 4-J-2: Operator Manual Table of Contents

8. Emergency Preparedness

- 8.1. Process Description
- 8.2. Safety and Health Considerations
- 8.3. Security Considerations**
- 8.4. Leak Detection
- 8.5. Emergency Response
- 8.6. Evacuation Detailed
- 8.7. Incident Command
- 8.8. Emergency Call Out Procedures

Page 125 changes

6-A: Update the Startup Execution Plan & Release for Construction

G. Basic Steps:

1. Review all significant project developments since the last update of the Startup Execution Plan (Activity 4-O), particularly developments pertaining to suppliers, spare parts, QA/QC, expediting, and construction plans and progress.
2. Expand and update the Startup Execution Plan as appropriate or needed.
3. Finalize the checkout/commissioning plan, the plan for initial operations, and the plan for the introduction of feedstocks, **including safety and security**.

Page 130 changes

6-F: Finalize the Startup Risk Assessment

E. Responsibility: Manufacturing Operations Representative, Startup Manager

Accountability: Contractor Project Manager

Consult: Business Unit Manager, Owner Project Manager, Construction Manager, Planner/Scheduler, Estimator, **Security Manager**

Inform: Plant Manager

F. Quality Gate/Sequencing Constraints: This activity is not a quality gate, but should be done prior to commissioning.

G. Basic Steps:

1. This activity should build on previous activity 4-I. Any recently discovered risks should be fully reviewed and strategies should be developed to minimize the risks. In particular, review the following: construction progress and available resources; changes; **security threat changes**; market issues; and QA/QC.

Page 155 changes

Security includes all measures taken to guard against malevolent, intentional acts, both internal and external (e.g., sabotage, crime, and attack), that result in adverse impacts such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and offsite effects (consequences).

Security Vulnerability Assessment: A continuous project lifecycle process in which the threat, critical assets, consequences of incident, physical security and risk are assessed.

3-X Plan for Startup Security

A. Phase: Front-end Engineering

B. Key Concepts: Startup Security risks must be assessed early-on in order to minimize their impact. Documented startup security lessons learned can be very helpful in this effort.

C. Deliverables: A listing of potential risks to successful startup security and associated estimates of impact. Updated SVA and updated security plan.

D. Motive/Rationale: Overlooked security risks can severely impact startup schedule, cost performance, and other measures of success. Early detection efforts are needed in order to reduce or contain these loss potentials.

E. Responsibility: Startup Manager

Accountability: Manufacturing Operations Representative, Owner Project Manager

Consult: Contractor Project Manager, Planner/Scheduler, Security Manager

Inform: Plant Manager

F. Quality Gate/Sequencing Constraints: This activity is not a quality gate, but should occur before approval of appropriation request.

G. Basic Steps:

1. Consult the Startup Execution Plan, Security Vulnerability Assessment, security plan, and lessons learned to date.
2. Identify risks associated with security concerns.

H. Tools Needed: Security Vulnerability Assessment, Process Hazards Analysis

I. Challenges to Successful Implementation:

- Obtaining accurate threat information with which to update SVA
- Budget limitations
- Understanding of operational environment (cultural, economic, social)
- Lack of security awareness
- Limitations of in-house expertise

4-X Update Startup Security Plan

A. Phase: Detailed Design

B. Key Concepts: The identification and assessment of startup security risks should be updated and refined in the detailed design phase.

C. Deliverables: An updated listing of potential risks to successful startup security and associated estimates of impact. Updated SVA and updated security plan.

D. Motive/Rationale: Overlooked security risks can severely impact startup schedule, cost performance, and other measures of success. Security situation is fluid; an update is essential to ensure accuracy.

E. Responsibility: Startup Manager

Accountability: Manufacturing Operations Representative, Owner Project Manager

Consult: Contractor Project Manager, Planner/Scheduler, Security Manager

Inform: Plant Manager

F. Quality Gate/Sequencing Constraints: This activity is not a quality gate, but should occur before completion of detailed design.

G. Basic Steps:

1. Consult the updated Startup Execution Plan, Security Vulnerability Assessment, security plan, and lessons learned to date.
2. Update risks associated with security concerns.
3. Propose and evaluate security strategies for implementation. Define contingency actions, complete with responsibility assignments.

H. Tools Needed: Security Vulnerability Assessment, Process Hazards Analysis

I. Challenges to Successful Implementation:

- Obtaining accurate threat information with which to update SVA
- Budget limitations
- Understanding of operational environment (cultural, economic, social)
- Lack of security awareness
- Limitations of in-house expertise

6-X Finalize Startup Security Plan

A. Phase: Construction

B. Key Concepts: The startup security plan developed during detailed design must be reviewed, updated, and communicated to the entire project team.

C. Deliverables: A final startup security plan delineating risk potential and critical risk abatement procedures.

D. Motive/Rationale: This is the final opportunity to mitigate security risk and to assure a safe startup through planning.

E. Responsibility: Startup Manager

Accountability: Manufacturing Operations Representative, Owner Project Manager

Consult: Contractor Project Manager, Planner/Scheduler, Security Manager

Inform: Plant Manager

F. Quality Gate/Sequencing Constraints: This activity is not a quality gate, but should occur prior to commissioning.

G. Basic Steps:

1. Consult the Startup Execution Plan, Security Vulnerability Assessment, security plan, and lessons learned to date.
2. Propose and evaluate security strategies for implementation. Define contingency actions, complete with responsibility assignments.
3. This activity should build on previous activity 4-X. Any recently discovered security risks should be fully reviewed and strategies should be developed to minimize the risks. In particular, review the following: the Startup Execution Plan, Security Vulnerability Assessment, security plan, and lessons learned to date.
4. Finalize plans for preventive or corrective action. Implement such action as appropriate.
5. Update documentation.

H. Tools Needed: Security Vulnerability Assessment, Process Hazards Analysis

I. Challenges to Successful Implementation:

- Obtaining accurate threat information with which to update SVA
- Budget limitations
- Understanding of operational environment (cultural, economic, social)
- Lack of security awareness
- Limitations of in-house expertise

Appendix K: Security Matrix

The Security Matrix below summarizes the updates of the best practices by project phase. "FEP" stands for Front-End Planning, "D" for Design, "P" for Procurement, "CON" for Construction and "SU" for Startup. The security updates are also organized by type of security that they address (Physical, Personnel or Information) and are colored to delineate between practices.

Phase	Physical	Personnel	Information
FEP	Security Stakeholders on P3 Team (AI #1)	Social Issues (B8)	CADD/Model Requirements (M1)
	Reliability Philosophy (A1)		
	Operating Philosophy (A3)	Training Requirements for Operational Facility (P6)	Document Control Systems (M3)
	Affordability/Feasibility (B4)		
	Affordability/Feasibility (7-3)		
	Future Expansion Considerations (B6)		
	Technology (C1)		
	Processes (C2)		
	Project Objectives Statement (D1)		
	Objectives with Security Delineated (AI #8)		
	Effective Communication (AI #4)		
	Clear Priorities (AI #3)		
	Project Design Criteria (D2)		
	Project Design Criteria (7-3)		

Phase	Physical	Personnel	Information
FEP	Site Characteristics (D3)		
	Lead/Discipline Scope of Work (D5)		
	Process Simplification (E1)		
	Design/Material Alternates Considered (E2)		
	Design/Material Alternates Considered (7-3)		
	Site Location (F1)		
	Site Location (7-3)		
	Permit Requirements (F4)		
	Fire Protection & Safety Considerations (F6)		
	Plot Plan (G8)		
	Plot Plan (7-3)		
	Equipment Status (H1)		
	Civil/Structural Requirements (I1)		
	Architectural Requirements (I2)		
	Water Treatment Requirements (J1)		
	Loading/Unloading/Storage Facilities Requirements (J2)		
	Substation Requirements		
	Power Sources Ident. (K4)		
	Instrument & Electrical Specifications (K6)		
	Procurement Procedures and Plans (L2)		
	Procurement/Logistics Procedures and Plans/Strategies (7-3)	Procurement/Logistics Procedures and Plans/Strategies (7-3)	Procurement/Logistics Procedures and Plans/Strategies (7-3)
	Engineering/Construction Plan & Approach (P2)		
	Engineering/Construction Plan & Approach (7-3)		
	Pre-Commiss. Turnover Sequence Requirements (P4)		

Phase	Physical	Personnel	Information
FEP	Startup Requirements (P5)		
	PEP incorporates security (I-1) - HIGH		
	PEP incorporates security (7-3)		
	Security input into planning (I-2) - HIGH		
	Security input into planning (7-3)	Security input into planning (7-3)	Security input into planning (7-3)
	Estimate Startup Security Costs (2-B)	Estimate Startup Security Costs (2-B)	Estimate Startup Security Costs (2-B)
	Resource Startup Security Costs (2-C)	Resource Startup Security Costs (2-C)	Resource Startup Security Costs (2-C)
	Identify Startup Security Objectives (3-A)	Identify Startup Security Objectives (3-A)	Identify Startup Security Objectives (3-A)
	Assign Startup Security Stakeholders (3-C)	Assign Startup Security Stakeholders (3-C)	Assign Startup Security Stakeholders (3-C)
	Reconcile Startup Logic with Security Plan (3-D)	Reconcile Startup Logic with Security Plan (3-D)	Reconcile Startup Logic with Security Plan (3-D)
	Acquire O&M Input for Security Systems (3-E)	Acquire O&M Input for Security Systems (3-E)	Acquire O&M Input for Security Systems (3-E)
	Identify Startup Security Risks (3-F)	Identify Startup Security Risks (3-F)	Identify Startup Security Risks (3-F)
	Identify Startup Security Procurement Requirements (3-H)	Identify Startup Security Procurement Requirements (3-H)	Identify Startup Security Procurement Requirements (3-H)
	Refine Startup Security Costs (3-I)	Refine Startup Security Costs (3-I)	Refine Startup Security Costs (3-I)
	Develop Startup Security Plan (3-X)	Develop Startup Security Plan (3-X)	Develop Startup Security Plan (3-X)
	Develop Construction Site Security Plan (JSS)	Develop Construction Site Security Plan (JSS)	Develop Construction Site Security Plan (JSS)

Phase	Physical	Personnel	Information
D	Design approaches and/or alternatives consider security (I-5) - HIGH; (II-2) - MED; (II-5) - MED Site layout considers security (I-6) - HIGH Consider security aspects of construction accessibility for retrofit (II-6) - HIGH Update Startup Security Risks (4-I) Ensure Security Addressed in O&M Training Plan (4-J) Refine Startup Security Costs (4-N) Update Startup Security Plan (4-X) Refine Construction Site Security Plan (JSS)		
		Update Startup Security Risks (4-I) Ensure Security Addressed in O&M Training Plan (4-J) Refine Startup Security Costs (4-N) Update Startup Security Plan (4-X) Refine Construction Site Security Plan (JSS) Design Effectiveness Criteria (RSB-1)	Update Startup Security Risks (4-I) Ensure Security Addressed in O&M Training Plan (4-J) Refine Startup Security Costs (4-N) Update Startup Security Plan (4-X) Refine Construction Site Security Plan (JSS)
P		Materials Management Personnel Security Procedures Training (7-3) Background Investigations/Personnel Screening for Site Personnel (7-3)	

Phase	Physical	Personnel	Information
CON	Assess & Communicate Startup Security Effects from Changes (4-B)	Assess & Communicate Startup Security Effects from Changes (4-B)	Assess & Communicate Startup Security Effects from Changes (4-B)
	Finalize Startup Security Risks (6-F)	Finalize Startup Security Risks (6-F)	Finalize Startup Security Risks (6-F)
	Finalize Startup Security Plan (6-X)	Finalize Startup Security Plan (6-X)	Finalize Startup Security Plan (6-X)
	Implement Construction Site Security Plan (7-3)	Implement Construction Site Security Plan (7-3)	Implement Construction Site Security Plan (7-3)
	Implement Construction Site Security Plan (JSS)	Implement Construction Site Security Plan (JSS)	Implement Construction Site Security Plan (JSS)
SU	Implement Startup Security Plan (7-A)	Implement Startup Security Plan (7-A)	Implement Startup Security Plan (7-A)
	Implement Construction Site Security Plan (JSS)	Implement Construction Site Security Plan (JSS)	Implement Construction Site Security Plan (JSS)

Appendix L: DoD UFC guidelines

The following guidelines are due to be published by the Department of Defense within the next five years.

- UFC 4-011-01: Security Engineering: Programming
- UFC 4-011-02: Security Engineering: Design
- UFC 4-012-01: Security Engineering: Design of Vehicle Access Control Points
- UFC 4-012-02: Security Engineering: Design and Selection of Vehicle Barriers
- UFC 4-012-03: Security Engineering: Design of Security Fencing, Gates, Barriers, and Guard Facilities
- UFC 4-012-04: Security Engineering: Structural Design to Resist Explosives Effects for New Buildings
- UFC 4-012-05: Security Engineering: Structural Design to Resist Explosives Effects for Existing Buildings
- UFC 4-012-06: Security Engineering: Design of Buildings to Resist Progressive Collapse
- UFC 4-012-07: Security Engineering: Design of Blast Resistant Windows and Doors
- UFC 4-012-08: Security Engineering: Design of Mail Rooms, Delivery Points, and Building Entrances to Resist Explosive Effects
- UFC 4-012-09: Security Engineering: Design to Resist Direct Fire Weapons Effects
- UFC 4-012-10: Security Engineering: Design of Safe Havens
- UFC 4-012-11: Security Engineering: Procedures for Designing Airborne Chemical, Biological, and Radiological Collective Protection for Buildings
- UFC 4-012-12: Security Engineering: Design Examples of Airborne Chemical, Biological, and Radiological Collective Protection Systems for Buildings
- UFC 4-012-13: Security Engineering: Airborne Chemical, Biological, and Radiological Detection Equipment Capabilities and Limitations
- UFC 4-012-14: Security Engineering: Airborne Chemical, Biological, and Radiological Particulate and Vapor Filtration Capabilities and Limitations
- UFC 4-012-15: Security Engineering: Design to Protect Against Waterborne Chemical, Biological, and Radiological Contaminants

Glossary

Alignment: the condition where appropriate project participants are working within acceptable tolerances to develop and meet a uniformly defined and understood set of project objectives

Consequence: the amount of loss or damage that can be expected, or may be expected from a successful attack against an asset

Constructability: the effective and timely integration of construction knowledge into the conceptual planning, design, construction and field operations of a project to achieve the overall project objectives in the best possible time and accuracy at the most cost-effective levels

Critical Infrastructure: the assets, systems, and functions vital to national security, governance, public health and safety, economy, and national morale

Design effectiveness: an all-encompassing term to measure the results of the design effort, including input variables and design execution, against the specified expectations of the owner

Domestic Terrorism: criminal acts dangerous to human life that appear intended to intimidate or coerce the civilian population or the government

Homeland Security: a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur

Information security: practices and procedures for protection of documents, networks, computer facilities and verbal communication. Firewalls, passwords, and a document control matrix are some examples of information security measures

Materials management: an integrated process for planning and controlling all necessary efforts to make certain that the quality and quantity of materials and equipment are appropriately specified in a timely manner, are obtained at a reasonable cost, and are available when needed

Personnel security: practices and procedures for hiring, terminations, and workplace issues and response

Physical security: involves equipment, building and grounds design and security practices designed to prevent physical attacks against facilities, people, property or information. Examples include fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass

Plant startup: the transitional phase between plant construction completion and commercial operations, including all of the activities that bridge these two phases

Pre-project planning: the process of developing sufficient strategic information with which owners can address risk and make decisions to commit resources in order to maximize the potential for a successful project

Security: includes all measures taken to guard against malevolent, intentional acts, both internal and external (e.g., sabotage, crime, and attack), that result in adverse impacts such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and offsite effects (consequence)

Security Vulnerability Assessment (SVA): the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact

Terrorism: premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience

Threat: any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset. It is also the intention and capability of an adversary to undertake actions that would be detrimental to valued assets

Bibliography

- American Chemistry Council. 2001. "Site Security Guidelines for the U.S. Chemical Industry" Hallcrest Systems, Inc.
- American Petroleum Institute and National Petrochemical & Refiners Association. 2003. "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries." API Publishing Services, Washington, DC.
- Brady, J.T., Spight, M.G., Thomas, S.R. and Lee, S. 2003. Job Site Security Guidelines.
- Bush, George W. 2002. Homeland Security Act of 2002. Webpage accessed at: <http://www.whitehouse.gov/deptofhomeland/analysis/>
- Bush, George W. 2002. The National Strategy for Homeland Security. Webpage accessed at: <http://www.whitehouse.gov/homeland/book/>
- Bush, George W. 2002. Securing the Homeland and Strengthening the Nation. Webpage accessed at: http://www.whitehouse.gov/homeland/homeland_security_book.html
- Bush, George W. 2003. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Webpage accessed at: http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf
- Center for Chemical Process Safety, American Institute of Chemical Engineers. 2002. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. New York
- Construction Industry Institute. 2002. Implementation of CII Best Practices IR 166-3. Austin, TX.
- Construction Industry Institute. 2001. A Guide to the CII Implementation Model and Knowledge Structure IR 166-2. Austin, TX.
- Construction Industry Institute. 1999. Procurement and Material Management: A Guide to Effective Project Execution IR 7-3. Austin, TX.

- Construction Industry Institute. 1998. Planning for Startup IR 121-2. Austin, TX.
- Construction Industry Institute. 1997. Alignment During Pre-Project Planning IR 113-3. Austin, TX.
- Construction Industry Institute. 1996. Project Definition Rating Index (PDRI), Industrial IR 113-2. Austin, TX.
- Construction Industry Institute. 1995. Pre-Project Planning Handbook SP 39-2. Austin, TX.
- Construction Industry Institute. 1993. Constructability Implementation Guide SP 34-1. Austin, TX.
- Construction Industry Institute. 1986. Constructability: A Primer Publication 3-1. Austin, TX.
- Construction Industry Institute. 1986. Design Effectiveness RS 8-1. Austin, TX.
- Council on Foreign Relations. 2003. "Terrorism: Questions & Answers" Homepage accessed at: <http://www.terrorismanswers.com/home/>
- Critical Infrastructure Protection Priorities Workshop. 2002. Proceedings from Conference held September 23, 2002. Washington, D.C.
- Department of Defense. 2002. UFC 4-010-01: DoD Minimum Antiterrorism Standards for Buildings
- Department of Homeland Security. 2003. Homepage accessed at: <http://www.dhs.gov/>
- Erwann, M.K. 2003. Working Paper #03-25 "New Challenges in Critical Infrastructures: A US Perspective." The Wharton School of the University of Pennsylvania.
- General Accounting Office. 2001, 2002, 2003. Special Collections – Homeland Security. Webpage accessed at: <http://www.gao.gov/homelandsecurity.html>
- Hartman, J. 2003. Conversation with Author, August 4, 2003. HQ US Army Corps of Engineers Engineering and Construction Building Systems Team Leader.

- Little, R., Meacham B., Smilowitz, R. 2002. "A Performance-Based Multi-Objective Decision Framework for Security and Natural Hazard Mitigation." Received from author.
- McFall, K. 2003. "Post 9/11 Investigations reveal Oil, Gas Achilles Heal." Engineer News Record. March 10, 2003 issue. Webpage accessed at: <http://www.construction.com/NewsCenter/Headlines/ENR/20030307b.asp>
- National Research Council, Committee on Science and Technology for Countering Terrorism. 2002. Making the Nation Safer: the Role of Science and Technology in Countering Terrorism. National Academy Press, Washington, D.C.
- Reuters. 2003. "Blackout blues: New York takes \$1 bn hit." August 19th, 8:15AM
- Rubin, C., Cumming, W., Renda-Tanali, I., and Birkland, T. 2003. "Major Terrorism Events and Their U.S. Outcomes (1988-2001)." Natural Hazards Research Working Paper #107. University of Colorado
- Sylvie, J. 2003. Microsoft Excel Chart of Best Practice Security Applicability and Impact. Received from author.
- Tamaki, J., Chong, J., and Landsberg, M. August 23, 2003. "Radicals Target SUVs in Series of Southland Attacks." Los Angeles Times.
- The Infrastructure Security Partnership. 2003. Homepage accessed at: <http://www.tisp.org/>
- Union Carbide Corporation. 2002. "Bhopal." Homepage accessed at: <http://www.bhopal.com/index.htm>
- World Nuclear Organization. 2003. "Information on Three Mile Island: 1979" Webpage accessed at: <http://www.world-nuclear.org/info/inf36.htm>